Compare Exchange Management Tools p. 40

Windows IT Pro

FEBRUARY 2009 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

IT IN THE CLOUD

Set Up, Deploy, and Manage Microsoft's Business Productivity Online Suite p. 15

Solutions Plus: Enable Wireless Security p. 20

Track AD Changes p. 25

Protect SharePoint with ISA Server p. 33

A Mobile Future: Smart Policies for Deployment p. 3

Troubleshoot Event Log Errors p. 9

Penton
A PENTON PUBLICATION
FEBRUARY 2009
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95


Your potential. Our passion.®
Microsoft®
M S C
MSC TORONTO
Mediterranean Shipping Company has discovered a new form of energy.
Mediterranean Shipping Company (MSC) is the second-largest container ship line in the world, with a database that tracks more than 210 billion transactions a year. The company recently upgraded its database to Microsoft® SQL Server® 2008, not only to handle this massive load, but also to simplify MSC's database administration and help ensure high availability. Which is like a new form of energy for MSC. See the whole story at SQLServerEnergy.com
Microsoft® SQL Server® 2008
To get the full MSC story on your phone, snap a picture of this tag. (Requires a free mobile app from http://gettag.mobi)

C O N T E N T S

Windows IT Pro
A PENTON PUBLICATION

FEBRUARY_2009
VOLUME_15
NO_2

ON THE WEB

Read these articles at www.windowsitpro.com.

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page. COVER ILLUSTRATION BY ROY SCOTT.

C O N T E N T S

COLUMNS

IN EVERY ISSUE

WRITING FOR *WINDOWS IT PRO*

Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS

Contact Walter Karl, Inc. at 2 Blue Hill Plaza, 3rd Floor, Pearl River, NY 10965 or www.walterkarl.com/mailings/pentonLD/index.html.

REPRINTS

Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

James

"Many IT pros are already facing compliance and policy questions about mobile device usage."

A Mobile Future

Balancing device management with policy compliance

I can't remember a time when so many disruptive technologies have affected the IT industry—and all at the same time. From virtualization and cloud computing to the plummeting costs of computer hardware and disk storage, it's an exciting time to be in IT. Another significant trend is the increasing adoption of smartphones, laptops, and other mobile tools and technologies.

The latest batch of smartphones to hit the consumer market—the Apple iPhone 3G, the T-Mobile G1 (aka the "Google Phone"), and the BlackBerry Storm—all raise the bar in terms of what a mobile device is capable of. And the trend toward increasing power and functionality in smartphones will only accelerate: A survey recently conducted by the Pew Internet & American Life Project (www.pewinternet.org) led to a prediction that "the mobile device will be the primary connection tool to the Internet for most people in the world in 2020." (You can view the entire report, "The Future of the Internet III," at www.pewinternet.org/pdfs/PIP_FutureInternet3.pdf.)

This information corroborates what many of us have seen with our own friends, family, and colleagues. How many people do you know who have given up a landline telephone for a mobile phone? And how many users have asked you about integrating their new iPhone 3G with the corporate IT infrastructure?

The iPhone has made perhaps the greatest inroads in the enterprise over the past year. In his web-exclusive article "Things I Overheard While Talking to My iPhone" (www.windowsitpro.com, InstantDoc ID 100709), Mark Minasi explains that the iPhone is "the first cell phone OS that understands that it works for you, not the other way around." Paul Robichaux is also impressed with the iPhone, but in "iPhone 3G" (December 2008, InstantDoc ID 100479), he points out that the device still has some room for improvement as a business tool: "Unfortunately, the iPhone just isn't up to par as a mobile enterprise email device. Windows Mobile 6.1's maturity gives it a clear edge."

Policies First

As IT pros receive pressure from executives and users to support a wider array of mobile devices, they must remember the importance of implementing standard policies for how those devices will integrate with their existing IT infrastructure. Many IT pros are already facing compliance and policy questions about mobile device usage.

A *Windows IT Pro* reader told one of my colleagues that integrating new mobile devices such as the iPhone into his corporate IT infrastructure is already leading to a discussion about corporate policy. "Questions about users being able to download movies, music, and games have come up from HR," the reader said. "[As well as] compliance [with our corporate IT policy] and users 'syncing' content of questionable nature (adult, pirated) onto devices."

With many IT shops facing mixed deployments of devices—including BlackBerrys, iPhones, and Windows Mobile–powered devices—creating a uniform policy for all of them can be difficult. A variety of new products are stepping in to help fill the gap: KACE Networks has released its KBOX iPhone Management Module, and Zenprise added iPhone support to Zenprise MobileManager 4.1. Although products can help you manage your mobile devices, having sound, consistent policies regarding their deployment, usage auditing, and security is even more important.

Virtualization to the Rescue?

With the large influx of mobile devices for personal and business use, a potential solution is to leverage virtualization technology to allow users to use one device for both personal and business needs, switching between relevant virtual phone profiles. VMware's Mobile Virtualization Platform promises to do just that, but it's at least a year from hitting the market. Regardless, virtualization technology could help ease the adoption of disparate mobile device types into an existing IT infrastructure.

What Do You Think?

As always, we'd love to get your take on where you think the industry is headed. Are you already embracing smartphones in your organization? Or are you waiting for the market to stabilize, leaders to emerge, or new technologies (e.g., Windows Mobile 7) to arrive before taking the plunge? Send me your thoughts, or visit the Mobile & Wireless section in the Windows IT Pro forums (tinyurl.com/966way) to join an open discussion on the topic.

InstantDoc ID 101134

JEFF JAMES (jjames@windowsitpro.com) is Editor-in-Chief, Web Content Strategist for Penton Media's IT Publishing Group. He specializes in server operating systems, systems management, and server virtualization.

- WDS Rocks
- SRPs Clarified
- DebugDiag
- ProLiant G4 or G5?

LETTERS@WINDOWSITPRO.COM

WDS Rocks

I want to thank Rhonda Layfield for her article "Using WDS with Windows Server 2008" (December 2008, InstantDoc ID 100439). I was indeed able to set up a Windows Deployment Services (WDS) server in about an hour—actually, just over an hour (but I was using a Windows Server 2003 box). I never really considered using WDS during our Windows Vista migration. I actually used most of the base components—ImageX and WinPE for capturing and applying images—but without the benefit of a WDS server. I thought WDS would essentially be Remote Installation Services (RIS) 2.0, and I was never happy with RIS 1, so I approached WDS with some trepidation. Now that I'm using it, I've found that it's a great product at the right price. Not only have I moved our Vista images to it, I've also started using it for the Windows XP images we have left over. It's a snap to use, and there's no RISprep or OSChooser to get in the way.

—Michael Dragone

Thanks Mike! WDS is one of the new deployment tools I'm most excited about. If you like WDS, you really need to learn about WDSUtil, a command-line utility that lets you tweak WDS in ways that aren't available to the GUI.

—Rhonda Layfield

SRPs Clarified

Darren Mar-Elia's article,"Securing Windows Desktops Using Group Policy" (November 2008, InstantDoc ID 100264) touches on Software Restriction Policies (SRPs). I was hoping you could confirm one thing for me: SRPs only *restrict* application use; they can't elevate rights. Correct? In other words, if a user doesn't have local administrative rights, you can't use an SRP to configure certain applications to run as an administrator?

—Richard Van Alstine

You're correct with respect to SRP's limitations. They can't elevate a process. A feature in Vista's SRP implementation—called Basic User—actually removes administrative tokens from an otherwise elevated process, but not the other way around.

—Darren Mar-Elia

After reading Darren Mar-Elia's November article, I have a question. If I use the System Services policy to change the service account password, will it update both the user account password (Active Directory—AD—or SAM database) and the service account password (Service Control Manager—SCM)?

—Aaron Rogers

The System Services policy doesn't update service account information. For that functionality, you'd have to use Group Policy Preferences' Services feature, which can do both of the things you've identified.

—Darren Mar-Elia

What Would Microsoft Support Do?

I'm really enjoying Michael Morales's "What Would Microsoft Do?" column, particularly the December installment, "Simplify Process Troubleshooting with DebugDiag" (InstantDoc ID 100577). As a freelance Windows administrator, I've been working with Microsoft products for 10 years. Occasionally, I run into a problem that ends with an Internet search telling me to debug something—and then I'm lost. I've tried looking into the debugging tools, but most of them seem incredibly difficult to use, or they give results that tell me absolutely nothing. So I end up looking for other solutions. Next time I run into a problem that requires debugging something, I'll grab one of your articles and try it the Microsoft way! Keep up the good work.

—Marco Brouwer

InstantDoc ID 101094

Virtualization Rematch

I read Michael Otey's "Virtualization Rematch" (December 2008, InstantDoc ID 100573), and I have a question. In a few months, I'll be implementing Hyper-V and Essential Business Server (EBS) 2008 on four servers running Windows Server 2008 64-Bit Edition. I'm currently researching HP ProLiant servers that are compatible with Server 2008 or Hyper-V or both. You mention using a ProLiant ML370 G4 to test the retail version of Hyper-V and the 64-bit Server 2008 Enterprise Edition. I was wondering if that information is correct. In my research, I found that—in general—only the G5 series is capable because of its support for Intel-VT, its No Execute feature, and its BIOS support for virtualization. The Windows Server Catalog doesn't list the G4 as capable of running Hyper-V. Am I missing something?

—Nick Kucharew

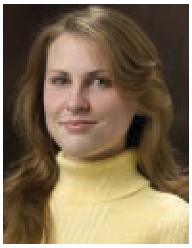
Yes. I used the rack-mounted HP ML370 G4, and it does support virtualization. However, if you're planning on running Hyper-V, you're correct to pay attention to the server's ability to support either the Intel-VT or AMD-V CPU virtualization feature set. Many servers today use the required x64 architecture but don't support hardware-assisted virtualization. The hardware vendors are aware of each system's ability to support virtualization, and you should be certain to verify this before you purchase your next server platform.

—Michael Otey

Oops!

On the November issue's Ctrl+Alt+Del page, we incorrectly attributed a tech quote to Anonymous. It was actually Robert Wilensy who wrote, "For years there has been a theory that millions of monkeys typing at random on millions of typewriters would reproduce the entire works of Shakespeare. The Internet has proven this theory to be untrue." Thanks to Dimitrios Kalemis for the correction!

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.



Humphries

The missing link to
IT resources

Green Means Go

Get started on green computing with *Windows IT Pro*

When it comes to being green, I can proudly say that my environmental consciousness is well maintained. I recycle everything that I can't reuse, bring my own shopping bags to the store, buy locally grown produce, suffer through teenagers' loud conversations about terrible music on my bus ride to work, and give an adequate amount of thought toward (maybe) starting my own compost pile. I find it quite easy to be green in my personal life, despite Kermit's thoughts on the matter. But when the hot topic "green computing" started popping up in office conversations like SUVs in the '90s, I saw a whole new perspective on being green.

Other than including one of those "Please consider the environment before printing this" images as part of my email signature, I hadn't really thought about how my work environment affected the planet's environment. Thankfully, the *Windows IT Pro* editorial team has a whole web page dedicated to the topic at WindowsITPro.com/GreenComputing.

According to Senior Editor Karen Bemowski, green computing refers to actions—such as consolidation and power management—that reduce IT departments' impact on the environment. In her August 2008 web-exclusive article "The Biggest Barriers to Going Green" (InstantDoc ID 99926), Karen references a CDW survey and explains that understanding *why* to implement green computing is fairly easy, but the *how* has stalled some organizations. "Although 80 percent of IT decision makers in government and corporate organizations believe that implementing green IT solutions is important, only 46 percent said their organizations were doing so."

Even if you're not personally interested in reducing your computing footprint, it's likely that related savings will interest company management. "IT Decision Makers Reveal Their Views on Going Green" (InstantDoc ID 99805) reports that "more than 70 percent of the IT decision makers [surveyed] said that they would probably or definitely increase their preference for purchasing green products if they were convinced there would be a positive effect on the environment and the business." And with savings of up to $73 per computer, as stated in "How Much Money Can We Save If We Use Power-Management Policies" (InstantDoc ID 100877), I'd say decision makers can easily find "positive effects."

So don't waste any more time (or energy). "Green up" your environment with the resources at WindowsITPro.com/GreenComputing.

InstantDoc ID 101062

What's On the Web in January

- Steps and best practices for transitioning to Exchange 2007 (InstantDoc ID 101071)
- Things we wish we'd known about Vista (InstantDoc ID 101072)
- Tips to help you become more proficient in Outlook (InstantDoc IDs 101095 and 101096)
- Using the audit policy subcategory "Special Logon" and changing a registry key using Group Policy Preferences (InstantDoc IDs 101060, 101061)

Find more free and VIP-only web articles at www.windowsitpro.com!

ONLINE

windowsitpro.com

Learn How to Reduce Downtime with CDP

Increased reliance on email means that any unscheduled downtime can quickly affect a company's bottom line. Traditional backup and recovery methods, which involve hours of downtime and unacceptable levels of data loss, no longer meet your needs. Read this Essential Guide to learn how to implement software-based continuous data protection (CDP) in your Exchange environment.

windowsitpro.com/go/ReduceDowntime

Keep SharePoint Growth in Check

Information archiving is a critical component of an effective SharePoint content life cycle management strategy. View this web seminar to explore Microsoft SQL Server capacity planning and recommendations for SharePoint, the performance and cost implications of unmanaged data growth versus effective content life cycle management, and archiving with DocAve Extension Archiver.

windowsitpro.com/go/SPGrowth

The Case for Disaster Recovery Planning and Budgeting

Justifying investment in an effective disaster recovery plan requires more than just warning about the dire consequences that may ensue if the company fails to act. Senior management needs a business case that spells out the costs and benefits of disaster recovery planning in terms that are relevant to the organization's financial performance. This web seminar will help you explain the real financial risks of various types of disasters and the costs required to address them.

windowsitpro.com/go/justifyingDR

Thurrott

"Windows 7 is dramatically faster than Vista and requires fewer hardware resources; it can run on netbook computers with just 1GB of RAM."

What You Need to Know About Windows 7 Beta 1

What I've seen of Windows 7 Beta 1 suggests to me that Microsoft has gotten its client OS mojo back again. The release seems to consist largely of changes for end users, improving the performance, stability, and reliability of the system, and it's already at roughly the quality point that Vista was when it launched more than two years ago. Here's what you need to know about Windows 7 Beta 1.

Changes for the Better

Overall, Windows 7 is dramatically faster than Vista and requires fewer hardware resources; it can run quite acceptably on small, low-end netbook computers with just 1GB of RAM, an impossibility for Vista. Boot and shutdown times have been cut considerably, as has the time it takes to resume from sleep mode, both of which lengthen battery life. And Windows 7 automatically shuts down network devices that are not in use, further improving battery life.

Many of the security improvements in Windows 7 will directly affect IT pros. For example, BitLocker has been improved with a new feature called BitLocker To Go that extends this encryption technology to portable storage. And User Account Control (UAC) has been significantly tweaked, appearing rarely and never flashing the annoying Secure Desktop anymore.

Close to the kernel, Microsoft has implemented its so-called Min-Win componentization scheme, isolating all low-level components of the system. Min-Win won't directly affect end users, but it does improve the reliability and stability of the system and gives Microsoft a level of process isolation that was previously impossible.

Windows 7 for End Users

The Windows desktop has been overhauled and sports new Aero glass effects. A new UI called Action Center replaces the old Security Center and adds PC-maintenance monitoring with centralized notifications. The Windows taskbar has been significantly overhauled and now works much like the Mac OS X Dock, mixing saved shortcuts with buttons for running applications and open windows. Also new to Windows 7 is a system of pop-up Jump Lists, which are specific to buttons on the taskbar; Microsoft supplies default options for each button, but developers can add application-specific options as well. Windows Explorer has evolved yet again with the return of the virtual-folder scheme that Microsoft briefly tried to implement in Vista. ReadyBoost, which improves system performance via caching on a USB thumb drive, now supports multiple memory devices and works with virtually any kind of removable storage, including Secure Digital cards.

Microsoft has also overhauled several Windows applications: Paint and WordPad adopt the Ribbon UI from Microsoft Office 2007, and Calculator supports multiple modes in addition to Standard and Scientific. The XML Paper Specification Viewer is improved, and a new PowerShell IDE is included. Most notable is that bundled applications such as Windows Contacts, Windows Calendar, and Windows Movie Maker are no longer included. Instead, users can download free and more frequently updated versions of these applications.

Windows 7 for the Enterprise

Microsoft is developing and shipping new client and server versions of Windows simultaneously (the server counterpart is Windows Server 2008 R2), with new features to make them work better together. For example, the search federation feature returns network-based searches quickly. Another feature, DirectAccess, makes difficult-to-configure and expensive-to-obtain VPN connections obsolete. (And for those who do stick with VPN, Windows 7 also includes a VPN Reconnect feature that automatically reconnects disconnected VPN connections.) BranchCache should improve network traffic between Windows 7 PCs in remote offices and Server 2008 R2–based servers in the main office.

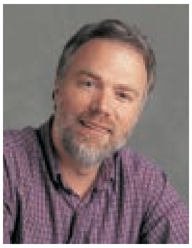
Windows 7 will ship with Windows PowerShell 2.0, as well as a powerful IDE. It also supports various virtualization technologies, including Virtual Hard Disk (VHD) mount and VHD boot.

Adopt or Not?

So should you wait for Windows 7 or adopt Vista? As of press time, Windows 7 should ship by early 2010, but my impressions of this beta release suggest that Windows 7 could ship by the third quarter of 2009 at the latest. Given that schedule, if you're not already migrating to Vista, yes, it does make sense to wait. And that's especially true if you're going to install the system on older hardware: Windows 7 runs much better than Vista on older PCs.

InstantDoc ID 101046

PAUL THURROTT (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).



Minasi

"With Forfiles, you essentially have a command-line version of Advanced Search."

Finishing Forfiles

Explore further functionality in the no-scripting scripting tool

Now that you know the basics of Forfiles (forfiles.exe)—a command-line tool that lets you perform repetitive tasks without having to learn how to script—it's time to delve deeper into Forfiles. Last month's "Forfiles Processes Scripts—Without Scripts!" (InstantDoc ID 100643) introduced four of Forfiles' most basic options: The /p option tells Forfiles what folder (or path) to use in its search; the /m option specifies which filenames to look for in that path; the /s option determines whether to also search subfolders; and the /d option lets you restrict the files that Forfiles operates on according to their date-modified value. Thus, the command

```
forfiles /p C:\windows /m *.exe
```

instructs Forfiles to display all .exe files in the C:\windows folder. Adding /s would instruct Forfiles to search C:\windows and all its subfolders for .exe files. (Vista has more than 19,000 of those subfolders, so think twice before trying that command!) And adding /d -100 further restricts the search to only those files modified in the past 100 days. But those four options are just the start!

Further Forfiles

Forfiles' greatest functionality lies in its /c option, which lets you control what to do with the files you find. For every file that meets your criteria, Forfiles stores information about that file in several built-in variables whose names all start with @ and contain the file's name (@file), extension (@ext), name without extension (@fname), full file specification (@path), date and time last modified (@fdate and @ftime), size in bytes (@fsize), and status as file or folder (@isdir). You can then use these variables to construct a command that performs a particular task on the selected files (e.g., display them, delete them, move them).

The default Forfiles /c command,

```
/c "cmd /c echo @file"
```

essentially displays just the filenames, making Forfiles a somewhat supercharged version of the Dir command. You can do more, however, by substituting your own /c options. For example, to delete all the .log files in the current folder, you could type

```
forfiles /m *.log /c "cmd /c del @file"
```

That functionality isn't terribly exciting, considering that the Del command has always accepted wildcards. But what if you wanted a Del command that deleted only log files that were larger than 1 million bytes? You could type

```
forfiles /m *.log /c "cmd /c IF @fsize GEQ 1000000
  (del @file)"
```

That example demonstrates the IF command that makes Forfiles shine. IF, a Windows command that lets you compare strings or numbers, uses the comparison operators EQU (is equal), NEQ (is not equal), LSS (is less than), LEQ (is less than or equal to), GTR (is greater than), and GEQ (is greater than or equal to). IF gets even more powerful with the addition of its partner ELSE. Suppose you want to delete all log files of 1 million bytes or more in size and move the rest to a folder named C:\logarchives. You could type

```
forfiles /m *.log /c "cmd /c IF @fsize GEQ 1000000
  (del @file) ELSE (move @file c:\logarchives)"
```

Notice a couple of points about the syntax. First, the command information following /c must be within double quotes. Second, when you use IF and ELSE, I recommend putting both the IF clause and the ELSE clause within parentheses to keep track of what you're telling the command to do. To clarify, here's another, simpler example. Suppose you want to create a simple listing of all the log files in the current folder, with each line listing the name of one file and a notation about whether that file is larger or smaller than a megabyte. That command would look like

```
forfiles /m *.log /c "cmd /c if @fsize GEQ 1000000
  (echo @file is a million bytes or larger.)
  ELSE (echo @file is under a million bytes in size.)"
```

Advanced Search

With Forfiles' ability to search on modification date and time and to report file size—along with a little IF/ELSE work—you now essentially have a command-line version of the Advanced Search capability that Windows Explorer has offered for the past few versions of Windows. That's what I call a useful tool.

InstantDoc 100440

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

TOP 8 CHALLENGES to MANAGING ENDPOINT SECURITY

Endpoint security is a veritable Medusa's head with seemingly unlimited attack vectors, each requiring specialized technology on multiple platforms. Taking on these risks one by one can quickly create an unwieldy and costly infrastructure. To address these risks without ruining productivity and driving up total cost of ownership, it is critical to take a holistic, coordinated approach. Make sure you understand the big picture before spending time and money solving an endpoint security problem.

1. Understanding all the risks

The risks associated with endpoint security cover all three fundamentals of information security: confidentiality, availability, and integrity. Endpoint devices like laptops and mobile devices inevitably store confidential information. Stolen endpoints or endpoints compromised by malware dominate media reports of accidental or malicious customer information disclosure incidents. But even if you can guarantee no confidential information resides on your endpoints, you still face risks associated with availability and integrity. Laptops and mobile devices that become unusable due to malware impact productivity, cause lost revenue, and increase support costs. And since endpoints are where most of an organization's information is initially captured and transactions initiated, compromised endpoint devices create a grave threat to the integrity of your business data.

2. Covering all attack vectors

Make sure you understand the difference between risks and attack vectors. While risks describe the negative business impact of a security incident to an organization – the "what" – attack vectors describe the "how" aspect of a security incident. And nowhere are there more attack vectors than with securing endpoints. Laptops can be attacked through a variety of physical access-related methods, including removal of storage and non-volatile memory, connection to ports, and installation of additional peripherals. Then there are removable media and removable storage devices. Malware in particular presents a constantly evolving mix of threats. You need to cover more than just viruses; it's paramount to fight all the types of new malware botnets, spyware, rootkits, etc. There are many "point" products that provide specialized mitigation against one specific attack vector, but the risk of addressing endpoint security risks with point products is that at the end of the day you've spent money on plugging your favorite security holes while leaving others untouched and you quickly find yourself underwater.

3. Endpoint security risks—and especially those related to malware—are not just a Windows problem anymore. The bad guys are paying more attention to Mac, Linux, and Unix. Servers of all types (Windows, Linux, Unix, etc.) require protection because endpoints communicate with all types of servers and can infect or be infected. And as more and more applications are pushed out to mobile devices, the platforms that must be secured grows and you can quickly find yourself as an organization depending on a new technology or platform without its protection in alignment with your organization's policies and security requirements.

4. Performance impact and user productivity
Many endpoint security operations—such as malware detection—are resource intensive, requiring CPU, memory, and disk. As you deploy more and more technologies to address various endpoint security risks, such technologies compete with each other for resources, leaving less and less for the actual applications users depend on to get their work done. Making the wheels of business grind to a halt in the interest of security is not a sustainable business model. Therefore, performance and capacity planning is just as much a part of endpoint technology requirements as any other technology implementation.

5. Total cost of ownership
Again, as you attempt to slay each serpent of the Medusa's head of endpoint security, another problem you may encounter with implementing too many "point" solutions is a fast-growing list of technologies to install, maintain, and keep licensed. If each product has its own arcane management interface and support caveats, your staff becomes spread too thin and TCO rises.

6. Historically, the Achilles' Heel of many endpoint security countermeasures has been dependence on user decisions such as warning the user before opening a potentially dangerous file. Users are trying to get their work done. Given the tension between productivity and security, it's not surprising that in study after study, given a choice users consistently fail to make good security decisions on their own.

7. Aligning endpoint technology controls with business requirements and policies
Endpoint devices have often been considered less important to security and security resources and compliance has been focused on servers and the network perimeter. But the trend in workstation/endpoint-related security bulletins from major software vendors like Microsoft, Apple, and others it's clear that endpoint security is just as relevant as any other component on your network, and security incidents at the endpoint are frequently compliance-related. Therefore, it's crucial to tie endpoint IT security policies back to approved corporate policy objectives, such as PCI or SOX.

8. Monitoring and verification
After deploying any security technology, you have to make sure it's healthy and effective. This is particularly difficult with endpoint security because of the quantity of systems involved and their mobile, frequently disconnected nature. To meet security and compliance requirements without losing control of costs, robust reporting and monitoring is imperative as you define the requirements for your overall endpoint security solution.

Morales

"Although troubleshooting event ID 333 errors can be tricky, there are ways to make the process easier."

Troubleshooting the Infamous Event ID 333 Errors

Use tips and Microsoft tools to diagnose and resolve these elusive errors

Windows Server 2003 SP1 introduced event ID 333 into the System event log. This particular event ID is quickly becoming one of the most frequent generators of Microsoft support calls—some of which have taken weeks to resolve. During such calls, we spend much time trying to figure out which general category the event 333 errors fall into. Because of its cryptic description, the error is time-consuming to diagnose and resolve. Here are some pointers for understanding event ID 333 errors, so that you can either solve the problem yourself or obtain information about it that will speed up a support call.

Event ID 333 Symptoms

Event ID 333's description is *An I/O operation initiated by the Registry failed unrecoverably. The Registry could not read in, write out, or flush, one of the files that contain the system's image of the Registry.* This means that the image of the registry held in memory could not be written to disk. Windows uses what's called the *lazy writer* to periodically write modified pages of memory to disk. When the lazy writer fails, an event ID 333 is recorded in the System event log.

The symptoms that might accompany event ID 333 errors include

- Server hangs: Your server may completely stop responding to keyboard or mouse movements and appears completely locked up, requiring a hard reboot.
- Server sluggishness: The server is extremely slow to respond at the console, and processing information is significantly delayed.
- Delayed Terminal Services connections: Users trying to log on to a terminal server could experience slow or delayed logons. Once they log on, they may be able to work without a slow experience; however, the logon takes several minutes instead of a few seconds.

Generally, event ID 333 can be classified into three categories:

- Memory resource depletion: When the lazy writer tried to write the modified pages in cache to disk, there weren't enough resources to complete the operation. This problem is often accompanied by event ID 2020 or 2019.
- Disk was too busy or inaccessible: Sometimes a busy disk might not respond quickly enough to handle the lazy writer's request to commit modified pages of memory to disk.
- Registry bloat: The registry suddenly grows in size, which makes it increasingly difficult for the lazy writer to commit the changes to disk. Registry bloat commonly occurs on terminal servers.

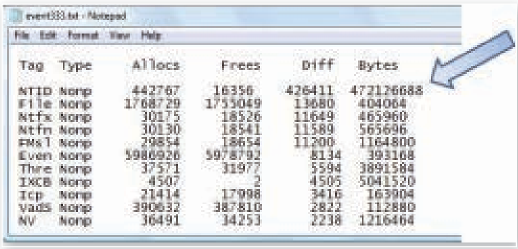
Especially frustrating is how the events continue to flood the System event log (many times per minute) until the server is rebooted. All it takes is one time for the lazy writer to fail for the event flooding to begin. Although the condition that caused the lazy writer to fail might have been brief (such as a short spike in memory usage), event ID 333 continues to be logged even during normal memory utilization. The event is still logged because the system recognizes that a failure to sync the registry has occurred and the registry version contained in memory is out of sync with the version on disk. As a result, the number and frequency of event ID 333 messages isn't a good indicator of the problem's severity. By default the lazy writer tries to flush to disk every five seconds.

Event ID 333 Troubleshooting Tools

When troubleshooting event ID 333 errors, first you must determine which general category the error falls into. Also it's useful to check the System event log for any other event IDs that accompany the 333 error, such as event ID 2020, which indicates a lack of paged pool memory, or event ID 2019, which indicates a leak in nonpaged pool memory.

These tools can help further diagnose event ID 333 messages:

- Performance Monitor: The counters to track are the system, memory, disk, and process objects.
- Memory object: Look for a rise in nonpaged or paged memory.
- Process object: Look for continuous rises in a process's handles just prior to the event ID 333's being logged.
- System object: The %Registry Quota In Use counter can be useful in displaying how much of the allowed registry quota is being utilized. The higher the percentage, the more likely that the problem is related to a growing registry.
- Physical disk: Look for increases in the Avg Disk Queue Length counter, which tracks the average number of read and write requests to the selected disk. If this counter spikes during the problem, start investigating the filter drivers (i.e., antivirus or backup software) on your system.
- Poolmon.exe: Included in the Windows Debugging Tools, Poolmon is used to track kernel pool memory usage by pool-allocation tag name. Using poolmon.exe can halve your trouble-



Tag	Type	Allocs	Frees	Diff	Bytes
NTID	Nonp	442767	16356	426411	472126688
File	Nonp	1768729	1755049	13680	404064
Ntfx	Nonp	30175	18526	11649	465960
Ntfn	Nonp	30130	18541	11589	565696
FMsl	Nonp	29854	18654	11200	1164800
Even	Nonp	5986926	5978792	8134	393168
Thre	Nonp	37571	31977	5594	3891584
IXCB	Nonp	4507	2	4505	5041520
Icp	Nonp	21414	17998	3416	163904
Vads	Nonp	390632	387810	2822	112880
NV	Nonp	36491	34253	2238	1216464

Figure 1: Poolmon.exe output indicating a leaking tag

```
Event Type: Warning
   Event Source: Userenv
   Event Category: None
   Event ID: 1517
   Date: Date
   Time: Time
   User: NT AUTHORITY\SYSTEM
   Computer: ComputerName
   Description:
Windows saved user User_Name
   registry while an application
or service was still using the
   registry during log off. The
   memory
used by the user's registry has not
   been freed. The registry will
be unloaded when it is no longer
   in use.
```

Figure 2: Event ID 1517

shooting time by enabling you to find the tag that's leaking memory.

- Dureg.exe: Dureg lets you view the size of the entire registry per hive. It's great for finding which registry hive is consuming the most space, which helps to determine what software might be causing the problem.

CASE 1: Finding a Memory-Leaking Driver

I recently worked on a problem where the customer's Windows 2003 SP2 server completely hung. Event 2019, *The server was unable to allocate from the system nonpaged pool because the pool was empty,* accompanied the 333 event and told me that this was a resource-depletion problem. The next step was to determine which driver was leaking. As Figure 1 shows, the output that Poolmon captured helped pinpoint which tag allocated the most memory. To help in quickly identifying the leaky tag, use the -b switch, which sorts the output based on byte usage for each tag. The tag at the top of the output is the one that's consumed the most memory (in bytes).

Our next step was to use Findstr to find the driver associated with the NTID tag:

```
C:\>findstr /m /s "NTID"
   *.sys
```

The /m switch tells Findstr to list only the filename in the output, and the /s switch searches in only the current folder and its subfolders. The Findstr output yielded the driver C:\WINDOWS\SYSTEM32\DRIVERS\CPQTEAM.SYS.

Our final step was to do a simple search on "NTID CPQTEAM". In the search results, we found a link to HP's tech forum that discussed a memory leak associated with a specific version of the Cpqteam .sys driver: forums13.itrc.hp.com/service/forums/questionanswer.do?admit=109447627+1227565774017+28353475&threadId=1147757.

CASE 2: Tracking Heavy Registry Usage

Not all event ID 333 errors are a result of a resource problem, however. It's possible to have event ID 333 errors and be unable to correlate them with any resource depletion. One such problem occurred on a Terminal Services server on which event ID 333 was flooding the System event log. Using Performance Monitor, we noticed that the counter %Registry Quota In Use was greater than 98 (i.e., the system was using more than 98 percent of the allowed system quota for the registry). Knowing that the system was heavily utilizing the registry, we took another look at the Application event log entries during the problem period and found event ID 1517, shown in Figure 2.

Event 1517 indicates that the registry isn't being freed when users log off. Our Performance Monitor counter %Registry Quota in Use correlates this information. We searched Microsoft Help and Support for "1517" and "registry" and found the article at support.microsoft.com/kb/944984, which fixed our problem.

Dureg.exe is another utility that's becoming increasingly popular for troubleshooting event ID 333 errors. Dureg.exe output needs to be collected once before users experience a problem and again during the problem period to determine whether the registry is becoming bloated. The first run of dureg.exe (before the problem) would look like this:

```
C:\>dureg.exe /a

Size of HKEY_CLASSES_ROOT : 11627272

Size of HKEY_USERS : 56739224
Size of HKEY_LOCAL_MACHINE : 47719408
Total Registry data size: 115985904
```

If you ran dureg.exe again when the slow-logon and event ID 333 problems are occurring, it would look like this:

```
C:\>dureg.exe /a
Size of HKEY_CLASSES_ROOT : 11879338
Size of HKEY_USERS : 335257592
Size of HKEY_LOCAL_MACHINE : 46006166
Total Registry data size: 392142994
```

Notice the large change in the HKEY_USERS key, from 56MB to 334MB. This information provides a valuable starting point for tech support that can drastically reduce the time needed to resolve the problem.

For this example, you'd want to run Regedit and navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software, then look for duplicate registry keys associated a particular application, because the values of this key are copied to a user's profile (HKEY_USERS) when the user logs on to a terminal server. An application might be flooding the Software key with values that end up bloating the registry and causing the Event ID 333 errors. Merely deleting any duplicate values under the HKEY_USERS key would be inadequate because the next time the user logged on, all those duplicate keys would be copied from the Software key to the HKEY_USERS key, and the problem would continue.

Faster Problem Solving

Troubleshooting Event ID 333 errors can be tricky, but now you have ways to make the process easier. By using the appropriate tools, you can more easily spot causes of Event ID 333 problems and use that information to resolve such problems faster.

InstantDoc ID 101059

MICHAEL MORALES (morales@microsoft.com) is a senior escalation engineer for Microsoft's Global Escalation Services team.

TOOL TIME

windowsitpro.com

Copy Many Pathnames at Once With Path Copy

Sometimes I need to put the pathnames of many files in a document. The traditional copy-and-paste methods let you copy only one pathname at a time, so I use Ninotech's Path Copy instead. This free utility lets you copy not only file paths but also folder and Universal Naming Convention (UNC) paths. Path Copy integrates with Windows Explorer, so it's there when you need it.

You can download Path Copy from the Simtel website (www.simtel.net/product.php[id]57104[sekid]0[SiteID]simtel.net). To install it, you unzip the files, right-click PATHC400.INF, and select Install. After installing Path Copy, a new context menu option named Copy Path appears when you highlight one or more items in Windows Explorer, and then right-click. When you select Copy Path, a submenu appears with several options. For folders and most file types, the available default options are Copy Long Path, Copy Long Name, Copy Long Folder, and Setup.

Let's say you have the mspdb60.dll and mspmsnsv.dll files highlighted in Windows Explorer. To copy their pathnames, you right-click, select Copy Path, then click Copy Long Path. The files' pathnames are now on the clipboard. To paste them, you press Ctrl+v (or right-click and select Paste) to get results such as

```
C:\WINDOWS\system32\mspdb60.dll
C:\WINDOWS\system32\mspmsnsv.dll
```

Selecting the Copy Long Name option produces the filenames (e.g., mspdb60.dll), whereas selecting the Copy Long Folder option provides the paths to the folder in which those files reside (e.g., C:\Windows\system32\).

You can use the Setup option to customize the submenu. Nine copy options are available. You can also create customized copy options. Path Copy works with Windows Vista, Windows XP, and Windows 2000.

—Serge Bedard, technology architecture specialist, CSST Quebec

InstantDoc ID 100962

■ Path Copy ■ Plink ■ SharePoint Manager ■ Remote Desktop

READER TO READER

Free Utility Makes Creating Custom Error Pages Easy in MOSS 2007

A task that Microsoft Office SharePoint Server 2007 (MOSS 2007) administrators often perform is to create a custom 404 error page to specify reporting or contact information to public users. The Microsoft article "How to point to a custom 404 error web page in Windows SharePoint Services 3.0 or in Microsoft Office SharePoint Server 2007" (support.microsoft.com/kb/941329) discusses how to create this page. One step involves using Microsoft Visual Studio 2005 to create a custom console application. However, not all administrators are trained in how to write a .NET application.

One workaround is to use the SharePoint Manager 2007 utility, which you can download from the CodePlex website (www.codeplex.com/spm). After you install this free utility on your MOSS 2007 machine, follow these steps to create a custom 404 error page:

1. Using an account that has administrative permissions, log on to your MOSS 2007 machine.

2. Open Windows Explorer. Navigate to the %SystemDrive%\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\TEMPLATE\LAYOUTS\LangID folder, where *LangID* is the ID of the language that you use. The language ID for US English is 1033.

3. In the LangID folder, create an HTML file that contains the reporting or contact information you want to provide to public users. This page can be as simple as

```
<HTML>
 <Body>
  <H1> Reporting or contact
   information goes here. </H1>
 </Body>
</HTML>
```

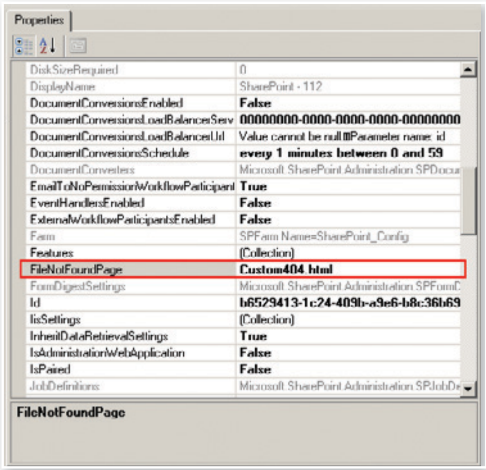


Figure 1: Updating the FileNotFoundPage property

4. Launch SharePoint Manager 2007 and connect to the SharePoint web application for which you're creating the error page.

5. Update the FileNotFoundPage property with the name of your HTML file. For example, if you named your file Custom404.html in step 3, you'd enter it as shown in Figure 1. After you update the property, click File, then select the *Save Changes to SharePoint* option.

6. To test your error page, launch Microsoft Internet Explorer (IE) and enter an invalid SharePoint URL, such as http://SharePointServer/aaaa.aspx. Your error page should appear.

—Jian Bo

InstantDoc ID 100958

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com. If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the InstantDoc ID text box.

Use Plink to Reboot VMware VMs

In our data center, we use VMware's Virtual Infrastructure 3.0. Recently, I was looking for a way to programmatically power cycle—in other words, turn off and then turn back on—a virtual machine (VM) from a remote Windows host. I came across a free utility named Plink, which is essentially a command-line interface for PuTTY, an open-source Secure Shell (SSH) and Telnet client.

I decided to try Plink. After I downloaded it from the PuTTY Download Page (www.chiark.greenend.org.uk/~sgtatham/putty/download.html), I used Plink to issue the command

```
plink.exe -load "ESXservername"
  -ssh -batch -l ESXusername
  -pw ESXpassword -m stopscript
```

where

- *ESXservername* is the name of the VMware ESX Server host on which the VM resides.
- *ESXusername* is the name of the account that has the right to power cycle the VM. (As a security precaution, this account should have only the right to power cycle specific VMs; it should have no other rights.)
- *ESXpassword* is the password for the account that has the right to power cycle the VM. (For better security, you can use public key encryption and store your private keys in a free associated application named Pageant available from the PuTTy Download Page.)
- *stopscript* is the name of text file that contains the shutdown commands to be executed.

The stopscript file contained the commands

```
/usr/bin/vmware-cmd /vmfs/
  volumes/DataStoreName/
  VMName/VMName.vmx stop
exit
```

where *DataStoreName* is the friendly name of the VMware File System (VMFS) data store and *VMName* is the name of the VM to shut down.

To start the VM back up, I used the command

```
plink.exe -load "ESXservername"
  -ssh -batch -l ESXusername
  -pw ESXpassword -m startscript
```

where *startscript* is the name of text file that contains the startup commands to be executed. Those commands were

```
/usr/bin/vmware-cmd /vmfs/
  volumes/DataStoreName/
  VMName/VMName.vmx start
exit
```

The ability to shut down and restart a guest OS gracefully has been extremely useful. It lets us programmatically reboot servers in isolated certification environments and power off VMs that are required only during certain hours. This method has proved more flexible than scheduling tasks in VMware vCenter Server (formerly VMware VirtualCenter) because we can use the scripts with third-party schedulers and in conjunction with other scheduled tasks, such as SAN replication. Overall, Plink has been an invaluable utility that has provided us an efficient means of programmatically accessing our ESX infrastructure.

—Brent McCraney, senior technical analyst, Ontario Teachers' Pension Plan

InstantDoc ID 100961

Registry Tweak Restores Connection to a Remote Windows 2008 Server

I recently faced a problem when trying to connect to a remote Windows Server 2008 server. I initially tried to connect with Remote Desktop Connection but was unsuccessful. Next, I tried to connect with the Microsoft Management Console Remote Desktops snap-in, but the session was immediately disconnected. A quick ping test revealed that the server was running, so I decided to see whether I could use the Server Message Block (SMB) protocol to connect to an administrative share (C$). That approach was successful.

Apostolos Fotakelis

Because the Server 2008 machine wasn't a critical server, I decided to use the Shutdown command from my desktop to remotely shut it down. After rebooting, I tried both the Remote Desktops snap-in and Remote Desktop Connection with no luck. However, this time I received the following error message that proved helpful: *The remote computer requires Network Level Authentication, which your computer does not support.*

I don't use Network Level Authentication (NLA), so my Server 2008 machines are configured to allow connections from computers running any version of Remote Desktop Connection. (Curiously, even Remote Desktop Connection 6.0 doesn't support NLA on Windows XP.) However, for a reason I couldn't figure out, my remote server had reconfigured itself to accept only NLA RDP connections.

Physically visiting the remote Server 2008 machine to reconfigure the relevant option wasn't feasible, so I searched for an alternative. After I investigated some solutions, I had an idea: I'd try to tweak the remote server's registry to change the option.

After some research on the Internet, I found a blog—"Programmatically Determining Terminal Server Mode on Windows Server 2008" (blogs.sepago.de/helge/2007/09/12/programmatically-determining-terminal-server-mode-on-windows-server-2008)—that discusses remote desktop registry settings. So I opened regedit and connected to the remote server's registry. I then navigated to HKLM\System\CurrentControlSet\Control\Terminal Server and verified that the fDenyTSConnections entry was already set to 0.

The SecurityLayer entry under HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp was already set to 1, but the UserAuthentication entry was also set to 1. That's the reason I couldn't connect. I changed the value to 0.

After making this registry tweak, I tried to connect the remote server. This time, I successfully made the connection.

—Apostolos Fotakelis, systems administrator, Aristotle University of Thessaloniki, and freelance IT consultant

InstantDoc ID 100981

- Backup
- Group Policy
- Disk management

ANSWERS TO YOUR QUESTIONS

Q: How can I restore Windows XP or Windows 2003 backups on a Windows Vista or Windows Server 2008 machine?

A: Microsoft's Windows NT Backup–Restore Utility (available at www.microsoft.com/downloads/details.aspx?FamilyID=7da725e2-8b69-4c65-afa3-2a53107d54a7) lets you restore XP and Windows 2003 backups to a Vista or Server 2008 machine.

Both 32-bit and 64-bit versions are available, and the only requirement is that you enable the Removable Storage Management feature. Instructions for enabling the Removable Storage Management feature are on the utility's website. For Vista, use the Control Panel's Turn Windows Features On or Off applet and enable Removable Storage Management. For Server 2008, use the Add Features Wizard and enable the Removable Storage Management feature.

—John Savill
InstantDoc ID 98863

Q: I've renamed servers using a special script but am now having problems accessing disks via the Microsoft Management Console (MMC) Disk Management snap-in. What's the problem?

A: A reader emailed me about a bug he discovered: When he renamed a server that has dynamic disks, upon reboot he could no longer access the disks via the MMC Disk Management snap-in. Instead of showing the disk content, the snap-in displayed the disk icons with a red X and no name.

I tried to reproduce this behavior but was unable to do so. I dug further and discovered that the cause of the problem was the rename: The name of the disk group in the HKLM\System\CurrentControlSet\Services\dmio\BootInfo\Disk Group registry subkey was the new server name (e.g., newnameDg0 instead of oldnameDg0), which didn't match the configuration that's stored at the end of the dynamic disk. To resolve the problem, I changed the name in the registry to the old server name, which allowed the Disk Management applet to function.

I learned that to rename the server, the user had used a script that searched and replaced server names in the registry rather than using the OS computer-rename functionality, which is why the dynamic disk information on the disk wasn't replaced.

The moral is therefore to not rename servers using registry search and replace. Instead, use the OS rename facilities. For example, you can use the netdom command or the Windows Management Instrumentation (WMI) Rename function of the computer object, as the following code illustrates:

```
strComputer = "."
Set objWMIService = _
  GetObject("winmgmts:" _
  & "{impersonationLevel=" _
  & "impersonate}!\\" _
  & strComputer & "\root\cimv2")
Set colComputers = _
  objWMIService.ExecQuery _
  ("Select * from" _
  & "Win32_ComputerSystem")
For Each objComputer in _
  colComputers
  errReturn = ObjComputer _
  .Rename("NewName")
  WScript.Echo "Computer name"_
 & "is now " & objComputer.Name
Next
```

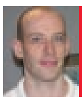
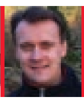
—John Savill
InstantDoc ID 95252

Q: In the Windows audit policy, an administrator can specify whether to log the success and/or failure events of different event categories (e.g., object access, logon/logoff). Does Windows provide a mechanism to define this audit policy more granularly, such as on a per-user basis? I want to specify an audit policy that logs only the failure logon/logoff events of the Administrator account. Currently, the most granular policy I can specify is to log the logon/logoff failures of all the accounts in the domain.

A: In Windows XP SP2 and Windows Server 2003, Microsoft introduced per-user auditing, which provides the functionality you're looking for. Per-user auditing is also supported in Windows Server 2008 and Windows Vista.

Per-user auditing lets an administrator define exceptions to the Windows audit policy (i.e., the audit policy you define in the Group Policy Object settings) on a per-user basis. However, exceptions can't be defined for the Administrator account or for members of the Administrators group. In fact, exceptions can't be defined for any groups—only for individual user accounts.

—Jan DeClercq
InstantDoc ID 98524

jsavill@windowsitpro.com
jan.declercq@hp.com

GET STARTED WITH Microsoft's Online Services

Deploy Exchange Online, SharePoint Online, and Microsoft Office Live Meeting in this series of easy steps

by Brett Hill

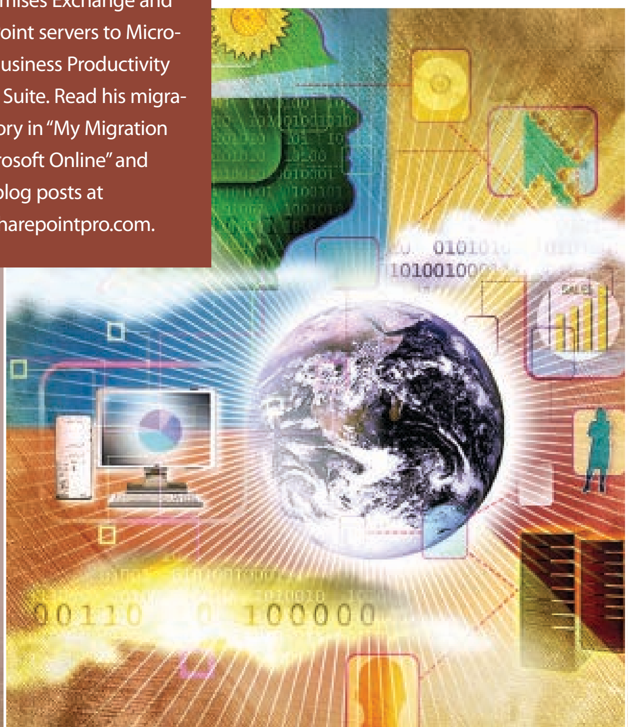
ILLUSTRATION BY ROY SCOTT

Real-World On-Premises to Online Migration

What's it like to move your major business applications into the cloud? *Windows IT Pro* contributing editor Dan Holme recently moved his on-premises Exchange and SharePoint servers to Microsoft's Business Productivity Online Suite. Read his migration story in "My Migration to Microsoft Online" and other blog posts at officesharepointpro.com.

If you've been paying even half attention to technology media in the past year, you've probably noticed that more vendors are trying to sell businesses on moving core IT operations to an Internet-based service-delivery mechanism—that is, cloud computing. Microsoft has been promoting a version of cloud computing, Software Plus Services (S+S). The heart of the difference between S+S and Software as a Service (SaaS) is that S+S uses specialized client-side software, such as Microsoft Office, in conjunction with online applications.

Microsoft's Business Productivity Online Suite (microsoft.com/online/business-productivity.mspx) is a great example of the kind of services that can have a big impact on small-to-midsized businesses (SMBs). A subscription to the Suite gives you access to Microsoft Exchange Online, Microsoft SharePoint Online, and Microsoft Office Live Meeting for $15 per user per month. Small-to-midsized businesses (SMBs) that would never consider having an on-premises Exchange server, for example, can now benefit from Microsoft Office Outlook features that "wake up" when used with Exchange (e.g., using the Global Address List—GAL, meeting-room scheduling, invitations to meetings with accept/deny built in, calendaring, and direct push email to Windows Mobile 6 devices). Similar capabilities are available from SharePoint Online for document collaboration and Live Meeting for real-time collaboration. Let's take an IT pro's-eye view of the Suite and walk through setting up the services.



Services Overview

The Suite comes in three flavors:

- Standard: This is the primary version of the Business Productivity Online Suite. At the Microsoft data center, these standard services are deployed using a *multi-tenant architecture* (i.e., a single instance of the software runs on the cloud vendor's servers, serving multiple client organizations, or tenants), which provides a very useful, affordable set of services. This model achieves scale and affordability by providing the most valuable core services while limiting the user's ability to customize the solution. Understanding the scope of what is and isn't customizable in the Standard version is key when you're evaluating or migrating to the Suite.
- Dedicated: Dedicated offerings, usually for businesses with at least 5,000 seats, are typically customized agreements that engage Microsoft to facilitate migration, support, and deployment. The dedicated version enables a greater degree of customization in multiple layers, such as supporting specific types of federated identity and SharePoint customizations.
- Deskless Worker: This is an inexpensive option for shop-floor workers or other scenarios that provides a mailbox accessible via Microsoft Outlook Web Access (OWA) and read-only SharePoint. This option is due for release the first half of 2009.

Subscribing to Microsoft Online Services

The Microsoft Online Customer Portal (MOCP, mocp.microsoftonline.com) is where you subscribe to services and add additional storage, if needed. Ordering the Business Productivity Online Suite is like ordering any other service: You provide your basic contact and company information and agree to the licensing and privacy terms. Here's how the signup procedure works.

1. Select a valid Windows Live ID to permanently associate with an MOCP account. The Live ID you select will be associated with the subscription you create. You can't use this ID for more than one subscription or change the Live ID association with the subscription. You'll use MOCP for adding more services or increasing storage, but not for day-to-day administration. Note that the Live ID can't be a username on the system, so you might want to create a special, new Live ID for the MOCP account.

2. Provide a good technical contact. The technical contact information you provide will receive communications about service updates and other service news. Microsoft support may also call or email this contact, if needed.

3. Provide the "base" domain name. The base domain name you provide will be added to microsoftonline.com to create a unique logon domain for your account. For example, if you enter contoso.com, your account will be provisioned as something similar to contoso1.microsoftonline.com. You can add a unique domain name to use for email and logon after your account is provisioned. Entering a domain during the signup doesn't affect any DNS server or impact mail routing for the entered domain.

4. Associate a partner. When you sign up, you'll be asked to select a Microsoft Partner to associate with your account. You can proceed without such an association, but Microsoft recommends working with a partner to help answer questions, plan migration, and integrate the services into your existing workflow.

5. Receive the Admin password. Once provisioned, you'll receive an email inviting you to return to MOCP and retrieve the Admin account password. Note that there's a delay at this stage while your account is provisioned. The provisioning process could take an entire day, but when I used the prerelease beta versions of Online Services, it took less time than this.

Figure 1: Microsoft Online Services Administration Center portal

With password in hand, you can now browse to the Microsoft Online Administration Center (MOAC, admin.microsoftonline.com), which Figure 1 shows, and start configuring the services.

Tips for New Subscribers

There are few actions an experienced services administrator (that's you) will want to take when a new account is provisioned. Following this advice will help you avoid reconfiguring settings later.

Add custom domains. *Before* you create new users, add and validate your main custom domain (click the Users tab, then click *Add a New Domain* from the Action List). To prevent fraudulent use of domain names, all


DON'T MESS WITH THE PBX.

custom domains used with the service must be validated. To validate a domain, you run the validation wizard, which provides you with a unique "string" that you then place into a CNAME of the authoritative DNS server for the domain. The domain validation wizard will then query DNS and examine the CNAME for the provided content. If there's a match, the domain is accepted. The assumption is that if you control the DNS server for your custom domain, you effectively own the domain. It's best if you reference the online Help for this process (www.microsoft.com/resources/Technet/en-us/MSOnline/bpos, and search for "verify a domain"), which does a good job of explaining it.

Once the domain is validated, set it as the default domain. Now proceed to create users. New users will automatically be assigned to the custom domain, so they log on as username@customdomain.com instead of username@customdomain1.microsoftonline.com. Note that you can't currently change the default logon domain for a user. Thus, if you created 100 users before you added a custom domain, they'd always have to log on as username@customdomain1.microsoftonline.com, until Microsoft changes this feature.

Create a new administrator that uses the services. Those of us used to managing OSs assign special meaning to the built-in Administrator account. With the Suite, the Admin account is like any other user account that's marked as service administrator. In other words, you can delete it or disable it without ill effects. I recommend that you create two administrator accounts, one that's provisioned for using all the services (i.e., one of your seats is consumed by this account) and a "backup" account that can be used for logging on and administering the services but isn't used as a service client. This backup account lets a second administrator gain access should the primary administrator be unavailable.

Configure Live Meeting settings. While logged on as Admin (and without the Sign-in application running; more about this shortly), launch Live Meeting from MOAC and configure the default settings for the Live Meeting administrator. Proceed to configure the Live Meeting profile for the Admin account. These settings will be used as the defaults for new Live Meeting users. If you set the defaults after users log on to Live Meeting, user settings aren't updated to reflect the changes because the profile has already been created. Settings to update include the maximum number of participants (15 maximum in the standard offering) and conference call/voice information, among others.

Creating and Managing Users

There are two types of users in the Suite: those you create in the administration center and those created by the Directory Synchronization tool. The process of creating users in MOAC is straightforward. Just start the New User Wizard from the Actions list on the main page and send the user the new password (which the user must change at the first logon). Note that you can also import multiple users using a .csv file.

You can download and install the Directory Synchronization tool in MOAC. The tool doesn't have a lot of administrative handles and is remarkably self-contained. Behind the scenes, the installer adds to the server Microsoft Identity Integration Server (MIIS), SQL Server 2005 Express Edition, and a Windows service that periodically replicates new accounts. Enterprise Administrator credentials are required to install the tool since it will crawl all domains in the forest for user objects.

When creating and managing users, here are some important things to keep in mind:

- An account will be created on the service for every user in the Active Directory (AD) forest. In the current version of the Directory Synchronization tool, you can't constrain the account to a specific organizational unit (OU) or domain.
- Passwords are not copied.
- New users created in AD will be replicated to the Suite, whereas users created in the service won't be replicated.
- Replicated accounts in the service aren't automatically provisioned with licenses; you must do so manually. This process is straightforward as you can select all unlicensed users at the same time and provision them.
- Replication occurs every 30 minutes by default. Event viewer messages tell you when sync starts and ends.
- You can kick off replication manually by running the Directory Synchronization tool.

Figure 2: Microsoft Online Services Sign-in application

Client Management

Client-side management tasks for the Suite include deploying the Sign-in application, performing some Outlook user-profile tweaking, and migrating email from your on-premises Exchange server to Exchange Online.

Sign-in application deployment. The Suite's Sign-in application is built to be deployed on subscriber desktops. As Figure 2 shows, you use the application to launch Outlook, OWA, SharePoint Online, and Live Meeting. In most cases, launching from the Sign-in application eliminates the need to manually authenticate to the services.

The Sign-in application is needed because user accounts for the service exist in Microsoft's data center and aren't part of the local company's AD or other membership system. As a result, the user ID and password are unique entities and don't share a security context with the signed-on user for the client system. As a customer, I like this because my company's local usernames and passwords aren't hosted inside Microsoft's data center. On the other hand, it would be convenient to have MIIS or another service as an option to bridge the identities. The initial release of the Standard Suite doesn't currently support federated identity.

As with any deployment, you'll need to assess the minimum hardware and software requirements; impact on user

Learning Path

Learn more about Microsoft's Business Productivity Online Suite:

Get Started with Business Productivity Online Standard Suite, technet.microsoft.com/en-us/library/cc742585.aspx

TechNet Webcast: Migration and Coexistence for the Business Productivity Online Suite..., msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032386692&CountryCode=US

Brett Hill's BPOSitive blog, blogs.technet.com/bpositive

Learn more about cloud computing:

Windows IT Pro Cloud Computing web page, windowsitpro.com/cloudcomputing

experience; and support, update, and installation requirements. The Sign-in application requires Windows XP Professional SP2 or Windows Vista Premium, Ultimate, or Enterprise. Microsoft .NET Framework 2.0 must be installed as the tool uses Windows Communication Foundation (WCF) to communicate to the service for authentication. Microsoft Office Outlook 2007 is supported as the email client. Finally, you'll need to be an administrator to install the tool. Download the tool from MOAC or home.microsoftonline.com.

Profile management. The Sign-in application will create a new Outlook user profile that connects Outlook to the Suite. Autodiscover works automatically in most cases (some tweaking may be needed in coexistence scenarios; check the online documentation for details), so that configuration is a seamless experience. You might need to perform certain administrative tasks associated with recovering autocomplete entries or adding a locally stored Inbox to the new profile. Both of these are straightforward tasks that you could automate if needed. Check out my blog entry (blogs.technet.com/bpositive) for more information about performing these tasks.

Email migration. The email migration tool moves email and related content to the Suite from Exchange. It also supports POP3 migration to a limited extent. Like the other tools, you can download this from MOAC and install it on a system that's joined to the AD forest. After you enter the services you're subscribed to and your Exchange admin credentials, the tool will query the Exchange server and find matching online accounts. You can then choose which users and content you want to migrate. For example, you could choose to migrate email in certain date ranges as well as journals, tasks, and other content associated with users' email accounts.

Once email is migrated to the online service, the user's AD account is set up with an alternate delivery address so that email directed to the local Exchange server is now routed to the service. The new online-services user will see a complete GAL (as a result of using the Directory Synchronization tool), will receive all mail from all sources, and can email any user without an interruption in service. Be aware that the migration tool doesn't migrate SharePoint content.

SharePoint Online

Service administrators can create SharePoint sites in MOAC. Doing so automatically makes the service admin who created the site an administrator on the SharePoint site. The first order of business, then, is to enter the SharePoint site and add SharePoint users.

Using SharePoint Online is much like using SharePoint on premises, except that the online version has some limitations due to the services' multi-tenant architecture. SharePoint Online is built on Microsoft Office SharePoint Server, so that a small business can benefit from publishing, collaboration, and Microsoft Office integration. Some SharePoint web services are exposed, which makes possible client-side custom applications and line-of-business integrations, such as those highlighted at the Partner Solutions Showcase (www.microsoft.com/online/partner/solutions-showcase.mspx).

Planning

Using the Business Productivity Online Suite is the easy part. Once you've deployed the solution, trained your users, and established your support systems, day-to-day operations should be easier for you than doing the same operations with on-premises servers. Getting there, however, requires some careful planning. You need to consider factors such as the impact of the online services on network bandwidth, reliability of your ISP, alternative Internet access plans, email migration planning, software upgrades, mobile-device configuration for email access (the Suite supports Windows Mobile 6 or later), DNS configuration, identification of service administrators, and updating support systems and network devices as required (e.g., content filtering, routers, proxies).

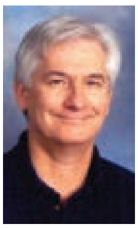
On the business side, you'll want to ensure that users are trained how to use the Sign-in application to launch Outlook and other services. For example, if you launch Outlook from the desktop icon instead of the Sign-in application dashboard, you'll be prompted to select the Outlook profile you want to use. Additionally, if the Sign-in application isn't running, you'll be prompted to authenticate and provide a client certificate. So make plans to inform users about these changes before deploying the Sign-in application.

To help with the planning process, the Microsoft Assessment and Planning (MAP) Toolkit (technet.microsoft.com/en-us/library/bb977556.aspx) has been updated to evaluate the on-premises systems for deploying the Suite. This set of questions and network query tool will provide useful information regarding impacts on bandwidth and currently installed versions of OSs and Office and includes checklists you can use to assess your preparation.

Now Try It Out!

Once you've deployed the Suite, routine server administration tasks are managed by Microsoft—so you might find yourself revisiting IT projects that you put on hold, now that you have time to do them. You can get a free trial account for Microsoft Online Services at mocp.microsoftonline.com. Take some time to review the online documentation, download the MAP toolkit, and get a feel for how the Suite works. I think you'll be impressed with the Suite's capability and ease of administration.

InstantDoc ID 101083



Brett Hill

(brett@iisanswers.com) is technical product manager at Microsoft in charge of technical readiness for Microsoft Partners with Microsoft Business Productivity Online Suite. He operates www.iistraining.com and maintains a blog at brettblog.com.

PROBLEM:

You need to implement a secure wireless LAN (WLAN).

SOLUTION:

Features in Windows Server 2008 and Windows Server 2003 provide everything you need, as long as you have three components in place: a compliant Access Point (AP), a compatible WLAN client, and an authentication server.

SOLUTION STEPS:

1. Install Internet Authentication Service (IAS).
2. Configure IAS as a Remote Authentication Dial-In User Service (RADIUS) server.
3. Configure the AP.

DIFFICULTY:

●●●○○

Enabling 802.11i WIRELESS SECURITY with Windows Servers

by Tom Carpenter

3 STEPS to securing your WLAN

Many small-to-midsized businesses (SMBs) struggle to budget for expensive wireless infrastructure equipment that's traditionally used in large organizations, even though SMB support teams seldom have the technical expertise needed to configure and maintain this complex hardware and software. Help is available, however: Features in Windows Server 2008 and Windows Server 2003 provide everything you need to implement a secure wireless LAN (WLAN). You need to have three components in place: a compliant Access Point (AP), a compatible WLAN client, and an authentication server.

First, let's examine the IEEE 802.11i standard for wireless security, then focus on the components, especially the authentication server component. I'll step you through how to install and configure your authentication server and show you how it fits into an 802.11i Robust Security Network (RSN) implementation.

How IEEE 802.11i Works

The IEEE 802.11i amendment to the 802.11 standard specifies security methods that leap far beyond those provided by the Wired Equivalent Privacy (WEP) standard. WEP was the security recommendation that was included in the original 1997 standard, and its weaknesses were quickly revealed. The security methods specified in IEEE 802.11i include the following.

IEEE 802.1X authentication. The IEEE 802.1X standard specifies methods used to implement port-based authentication. Port-based authentication is an authentication process that allows only credential exchanges to traverse the network until the user or machine connected to the port is authenticated. The port is called an uncontrolled port during the time in which it allows only credential exchanges. The port is called a controlled port after authentication is completed. This use of terms may seem counterintuitive, but the language is based on the concept of two virtual ports existing within a single physical port, or WLAN association, in the case of a wireless link. Devices compatible with 802.1X use the Extensible Authentication Protocol (EAP) for authentication and to move the port from the uncontrolled (unauthorized) to the controlled (authorized) state. The fundamental concept of EAP is that it's

extensible, meaning that authentication can be handled in different ways and there are several different EAP types. To learn more about the various EAP types you should or shouldn't use, see the sidebar "EAP Types."

TKIP and AES-CCMP key management. The Temporal Key Integrity Protocol (TKIP) is recommended as a transitional security protocol for older WLANs. So long as client devices support Advanced Encryption Standard (AES) with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for key management, as most new hardware and software does, a newly implemented WLAN will most likely use AES-CCMP. TKIP and AES-CCMP are used to exchange encryption keys in a secure manner. Both group encryption keys, which are used for broadcast and multicast messages, and private encryption keys must be generated and managed.

RC4 and AES encryption. After the authentication is complete and the encryption keys are implemented, those keys are used with either the RC4 (in the case of TKIP) or AES (in the case of CCMP) encryption algorithms. These encryption algorithms protect the data as it travels across the wireless medium.

How Internet Authentication Service and RADIUS Work

Now let's look at the three components that must be in place for a secure WLAN: a compliant AP, a compatible WLAN client, and an authentication server. Most APs support 802.11i with the use of TKIP at a minimum, and more APs support AES-CCMP than ever before. As for compatible clients, both Windows Vista and Windows XP can function as RSN clients. RSN dynamically negotiates the authentication and encryption algorithms to be used for communications between wireless APs and wireless clients. Lastly, the core of an 802.11i authentication infrastructure is the authentication server, which is often built in to expensive WLAN infrastructure devices such as WLAN controllers.

In most implementations, the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server. Microsoft's RADIUS server is the Internet Authentication Service (IAS) in Windows 2003 and Windows 2003 R2. Server 2008 introduces Network Policy Server as the replacement for IAS and many other network services.

In 802.1X terminology, the IAS server plays the role of the authentication server. The AP plays the role of authenticator, and the client plays the role of supplicant. Figure 1, page 22, shows their relationship. The supplicant requests access to the network, and the authenticator (the AP) responds by requiring authentication. The supplicant provides credentials for the selected EAP type and sends them to the authenticator. The authenticator then forwards the credentials to the authentication server, IAS, which can request additional information from the supplicant. Eventually, the supplicant is either authenticated or rejected.

Step 1: Install IAS

IAS isn't installed by default on Windows 2003 servers. You need to add the service through the Control Panel *Add or Remove Programs* applet. Select the Add/Remove Windows Components button. In the Windows Components Wizard window, select the Networking Services components and

EAP Types

The IEEE 802.11 standard as amended (including the 802.11i amendment) doesn't dictate the Extensible Authentication Protocol (EAP) type that should be used. However, it does suggest that you use an EAP type supporting mutual authentication to implement Robust Security Network (RSN) associations, which are logical connections between wireless clients and the network infrastructure APs. Table A compares the different EAP types and their capabilities and recommends whether they should be used in production networks.

Of the three EAP types supported by Windows Server 2003, only EAP-Transport Layer Security (EAP-TLS) and Protected Extensible Authentication Protocol (PEAP) should be used in a production environment. EAP-Message Digest 5 (EAP-MD5) uses very weak authentication algorithms and should be used only for initial testing of a Remote Authentication Dial-In User Service (RADIUS) server.

Whether you choose to use EAP-TLS or PEAP, the RADIUS server will need a certificate. This certificate can be provided by the Certificate Services server available with Windows servers. You'll need to implement a public key infrastructure (PKI) solution if you plan to use EAP-TLS because the clients (end nodes, in this case) as well as the RADIUS server need to have certificates. PEAP requires only the server-side certificate. An out-of-the-box installation of IAS provides only PEAP and EAP-MD5 for wireless remote access policies.

Table A: EAP Types and Suitability for Production Network Use

Authentication/ Authorization Capabilities	EAP-MD5	EAP-TLS	PEAP
Certificates – Client	No	Yes	No (Microsoft Challenge Handshake Authentication Protocol—MSCHAP—V2), Yes (TLS)
Certificates – Server	No	Yes	Yes (all)
Password Authentication for Clients	No	No	Yes (MSCHAP V2), No (TLS)
Protected Access Credentials Used	No	No	No
Credential Protection	Weak	Strong	Strong
Encryption Key Management	No	Yes	Yes
Mutual Authentication	No	Yes	Yes
Recommended for Production	No	Yes	Yes

Figure 1: The authentication process

click the Details button. From here, select the Internet Authentication Services subcomponent, then click OK. Click Next to continue with the installation, then click Finish to complete the installation. During this process, you might be asked for the installation media. If requested, provide the appropriate Windows 2003 disks.

Additionally, you need an enterprise root certification authority to be able to install and configure IAS properly. If you've studied public key infrastructure (PKI) implementations in Windows environments, you'll know that this constraint imposes the need for a Windows domain. However, if you're implementing RADIUS through IAS, you're likely to be running a Windows domain and shouldn't have a problem.

Step 2: Configure IAS

Assuming the default logging properties are acceptable to you, the first thing you must do is configure the clients of the RADIUS or IAS server. Although you might typically think of clients as end nodes on your network, RADIUS-based authentication architectures are different. The end nodes connect to the APs as clients, and the APs connect to the RADIUS server as clients. Therefore, the clients you need to configure in the IAS configuration tool are the APs used in your WLAN.

To begin configuring clients of the IAS service, click Start and navigate to Administrative Tools, Internet Authentication Service. After the IAS manager loads, you'll see a screen like that in Figure 2. Right-click the RADIUS Clients node and select New RADIUS Client. You'll need to provide the following information:

- friendly name
- client address
- client-vendor
- shared secret

The friendly-name parameter can be any letters or digits you desire; names like WAP1 and WAP2 always work well for me. The client address can be either the DNS name or the IP address. In most cases, you'll choose to use the IP address since APs are often implemented without names. The client-vendor setting will usually be configured as the default of RADIUS Standard, which is compatible with most RADIUS devices; however, to take advantage of some vendors' proprietary enhancements, you might need to select the appropriate vendor. Finally, the shared secret is used to secure the communications between the AP and the RADIUS server. Be sure to use a strong passphrase that includes uppercase letters, lowercase letters, and digits, to ensure that the RADIUS communications across the wired side of the network are secure.

After you create the client configuration settings, the next step is to configure a remote-access policy to control the allowed authentication methods. Create this policy by right-clicking Remote Access Policies and selecting New Access Policy. Click Next in the wizard to begin creating the policy. From here, you can either use a wizard to create a standard policy or you can create a custom policy with full control over all EAP and RADIUS messages. The policy should be given a name that reflects its purpose. I often choose names such as EAP-TLS Authentication or EAP-TTLS Authentication.

Step 3: Configure the AP

The final step in this process is to configure the AP to use the RADIUS server to authenticate WLAN clients. The procedure will vary according to the AP model and firmware version. However, the processes are similar:

1. Choose the section of the configuration interface that's related to security.
2. Select WPA-Enterprise or WPA2-Enterprise as the authentication method.

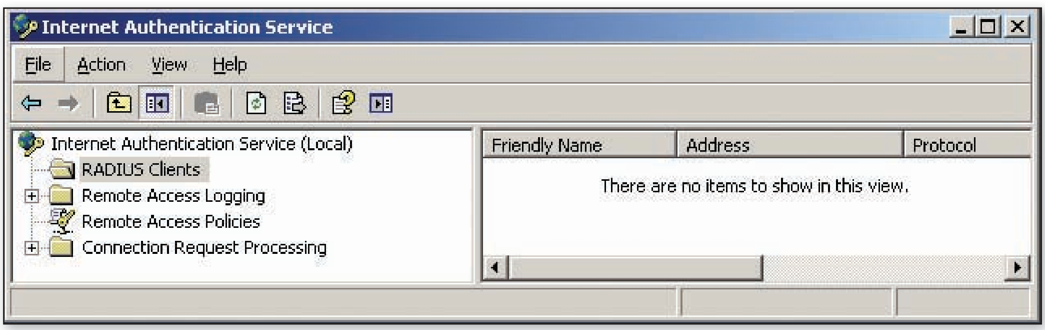


Figure 2: IAS manager screen

To advertise on this page, contact sales@windowsitpro.com or 800.621.1544

Features in Windows Server 2008 and Windows Server 2003 provide everything you need to implement a secure wireless LAN (WLAN).

3. Enter the IP address of the IAS server in the RADIUS server attribute field.

4. Enter the shared secret that you created when you created the RADIUS client for the AP in IAS.

After you complete these steps, the AP should be able to forward authentication requests from WLAN clients to the wired-side IAS/RADIUS server. Remember, the supplicant submits requests to the AP, which forwards them to the RADIUS server. Consequently, the AP effectively acts as a mediator between the clients and the RADIUS server, eliminating the need for WLAN clients to be RADIUS-server–aware.

A Commitment to RADIUS Authentication

Server 2008 introduces support for new EAP types, including EAP-Tunneled Transport Layer Security (EAP-TTLS), Light Extensible Authentication Protocol (LEAP), and EAP Flexible Authentication via Secure Tunneling (EAP-FAST, a secure replacement for Cisco's LEAP). These changes show Microsoft's commitment to continued support of RADIUS authentication in Windows Server.

Regardless of the RADIUS solution you select, the core of a solid 802.11i implementation is the PKI. The configuration of the infrastructure is fast and easy as long as you have a PKI in place. (For information about installing a PKI, see the Microsoft article "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure, at technet.microsoft.com/en-us/library/cc772670.aspx.) The good news is that implementing a PKI in Windows is a simple task; however, it's one that calls for thorough planning.

InstantDoc ID 98796

Tom Carpenter (carpenter@sysedco.com), senior consultant for SYSEDCO, is a trainer and consultant who has taught more than 30,000 IT professionals in the past 10 years. He's the author of numerous books, including *SQL Server 2005 Implementation and Maintenance* (McGraw-Hill).

CIO • CTO • DIRECTOR • ARCHITECT • ANALYST • CONSULTANT • VISIONARY

STRATEGIES DEFINED

PROBLEMS SOLVED

MARCH 15-18, 2009 • ORLANDO, FL
HYATT REGENCY GRAND CYPRESS

The cutting edge event for IT Professionals.

Attend dynamic Microsoft keynotes & get the scoop on the future trends in our industry!

Beyond the Hype, behind the scenes.
WinConnections brings the nation's top experts together to dive deep into the platforms and products you design, implement, and support, today and tomorrow.

- Train with Microsoft and industry experts delivering over 85+ in-depth sessions!

- Unwind in Orlando and make new friends.... Choose from many area attractions.

- Enter the raffle to win a 1 week cruise for two! Enter to win in the Expo Hall.

- Visit the cabana sessions in the expo hall. Meet and interact with authors and speakers.

TECHNICAL TAKEAWAYS

- Use Terminal Services in Windows Server 2008 to deploy more easily, improve printing, and improve security of your applications
- Voice-Enable your OCS 2007 R2 Deployment
- Adding and deploying images via WDS
- Integrate Exchange Unified Messaging with Office Communications Server 2007
- Deploying Exchange 2007 with Windows 2008 Hyper-V
- Plan for disaster recovery with your SharePoint sites
- NAP: Protection built into 2008
- Use Windows 2008 technologies to secure remote offices that lack a true data center
- Learn how to work with file shares in SharePoint

WHAT'S HAPPENING? SCHEDULE AT A GLANCE

SATURDAY, MARCH 14, 2009	
9:00am - 4:00pm	Pre-Conference Workshops
SUNDAY, MARCH 15, 2009	
9:00am - 4:00pm	Pre-Conference Workshops
6:30pm	Microsoft Keynote
(immediately following)	Opening Reception in Expo Hall
MONDAY, MARCH 16, 2009 • MICROSOFT DAY	
8:30am - 9:30am	Keynote
10:15am - 1:00pm	Conference Sessions
1:00pm - 2:30pm	Lunch/Expo Hall
2:30pm - 5:30pm	Conference Sessions
TUESDAY, MARCH 17, 2009	
8:30am - 1:00pm	Conference Sessions
1:00pm - 2:30pm	Lunch
2:15pm	Cruise Raffle *Must be present to win!*
2:30pm - 5:30pm	Conference Sessions
WEDNESDAY, MARCH 18, 2008	
8:00am - 12:30pm	Conference Sessions
12:30pm - 2:00pm	Lunch
2:00pm - 3:00pm	Conference Sessions
3:30pm - 4:15pm	Closing Q&A
THURSDAY, MARCH 19, 2008	

SEE WEB SITE FOR THE LATEST UPDATES • www.WinConnections.com

IT PROFESSIONAL • ADMINISTRATOR • ENGINEER • TECHNICIAN • EXPERT

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

STEVE RILEY MICROSOFT
How IT Will Change in the Next 10 Years and Why You Should Care

Steve Riley replaces the batteries in his crystal ball and takes a look at some predictable and not-so-predictable trends that you should prepare for now. Digital natives, the generation of people who you will soon be hiring, live in and expect something completely different than anything you've built or experienced so far. And yes, your career depends on them—so get yourself ready.

Steve Riley's career at Microsoft began in 1998 in the telecommunications practice of Microsoft Consulting Services where he worked with several ISPs and ASPs to design highly-available network architectures, develop hosting platforms for various custom and off-the-shelf applications, and deploy complex multi-site VPNs. His specialization in security led him next to the security consulting practice, where he worked with many customers to conduct security assessments and risk analysis, deploy technologies for attack prevention and intrusion detection, and assist with occasional incident response efforts. Steve is now a product manager in Microsoft's Security Business Unit. He is a frequent and popular speaker at conferences worldwide, often appearing in Asia one week and Europe the next; Steve's speaking engagements have included multiple Microsoft TechEds and other conferences, plus SANS, RSA, Black Hat, Windows IT Pro roadshows, and InfoSec US. When not evangelizing the benefits of Microsoft security technology, Steve spends time with customers to better understand the security pain they face and show how some of that pain can be eliminated. Steve's technical specialties include network and host security, communication protocols, network design, and information security policies and process.

MARK MINASI MR&D • *The Next Windows... Lucky Seven?*

Two years sooner than originally planned, Microsoft intends to ship the next Windows – the sequels to Vista and Server 2008 – in under two years in the mid-2010 time frame. Additionally, Redmond will, for the first time in ten years, ship both the desktop version and server version of Windows (generically known as "Windows Seven") at the same time.

Will Windows Seven capture buyer interest in a way that Vista could not? Well, there's some neat stuff in there, including tons of new application compatibility, niftier virtualization features (including a VMotion competitor), even more improvements in their deployment tools, tons of PowerShell-ability, security features that actually make getting to company resources easier than before, and of course there are the inevitable changes to the user interface. But will it be good enough to make you move from XP and 2003? Get the skinny so you can get ready for Windows Seven from independent industry watcher and Windows watcher Mark Minasi!

Mark Minasi is an author, a technology columnist, a commentator, a keynote speaker, and an all-around alpha geek. What separates him from many of the other alpha geeks is that he knows how to explain things to normal humans and often make them laugh while doing it. He's probably best known for his books, ***Mastering Windows NT Server*** (Sybex), ***Mastering Windows 2000 Server***, and ***The Complete PC Upgrade and Maintenance Guide*** and his columns in ***Windows IT Pro***. Mark has also authored 17 other technology books, spoken on technical topics in 20 countries, and written and appeared in a dozen technical education videos. His most recent works are ***Mastering Windows 2000 Server***, Third Edition and ***Mastering Windows XP Professional***. He has also written ***Linux for NT/2000 Administrators*** and a seventh edition of ***Mastering Windows NT Server 4.0***.

FRANCOIS AJENSTAT MICROSOFT • *Sustainable IT within Reach*

Environmental sustainability is a serious challenge that requires a comprehensive and global response from all sectors of society. Amid growing awareness about global climate change and the scarcity of resources, businesses worldwide are looking for ways to reduce their environmental footprint. Reducing energy use and rethinking business processes can increase profits and help companies more effectively lower their environmental footprint. It can also help their standing with environmentally aware business partners, investors and customers. In today's world, "going green" isn't just good for the planet, it's good for business. In this session, you will learn how you can reduce the environmental impact of IT; help manage your environmental footprint and initiatives; and provide ways to rethink business practices to reduce your environmental impact.

Francois Ajenstat is the Director of Environmental Sustainability at Microsoft Corp. He is responsible for Microsoft's communication and outreach for key sustainability initiatives across Technology and Innovation; Global Partnerships and Corporate Environmental Practices. Ajenstat has been at Microsoft for the past eight years in various groups, including the Server and Tools and Information Worker divisions and the Enterprise and Partner group. Before joining Microsoft, he worked at Cognos Inc. as a strategic alliance manager responsible for key technology partners.

Ajenstat received a computer science degree from the University of Ottawa in Canada. In his free time, he is an avid fan of architecture and interior design, as well as cycling and sailing.

SESSIONS PRESENTED BY MICROSOFT

ADVANCED WINDOWS POWERSHELL SCRIPTING
MICROSOFT

WINDOWS SERVER 2008 ACTIVE DIRECTORY FUNDAMENTALS
MICROSOFT

WINDOWS SERVER 2008 R2 OVERVIEW
MICROSOFT

CLUSTERING WINDOWS SERVER? SIMPLE!? YES!!!
MICROSOFT

INTRODUCTION TO HYPER-V IN WINDOWS SERVER 2008
MICROSOFT

HOW TO ELIMINATE THOSE PESKY LOGON DCRIPTS (AND MORE!) WITH GROUP POLICY PREFERENCES
MICROSOFT

WINDOWS SERVER 2008 R2 IIS 7.0 OVERVIEW
MICROSOFT

MANAGING HYPER-V USING POWERSHELL
MICROSOFT

WINDOWS 7 OVERVIEW
MICROSOFT

BUILDING A CASE FOR WINDOWS VISTA - THE ROAD FROM XP TO WINDOWS 7
MICROSOFT

ADVANCED DEPLOYMENT SCENARIOS WITH VISTA AND SCCM
MICROSOFT

MANAGING WINDOWS VISTA WITH POWERSHELL
MICROSOFT

Please Visit Web site for Microsoft Day Session Abstracts!

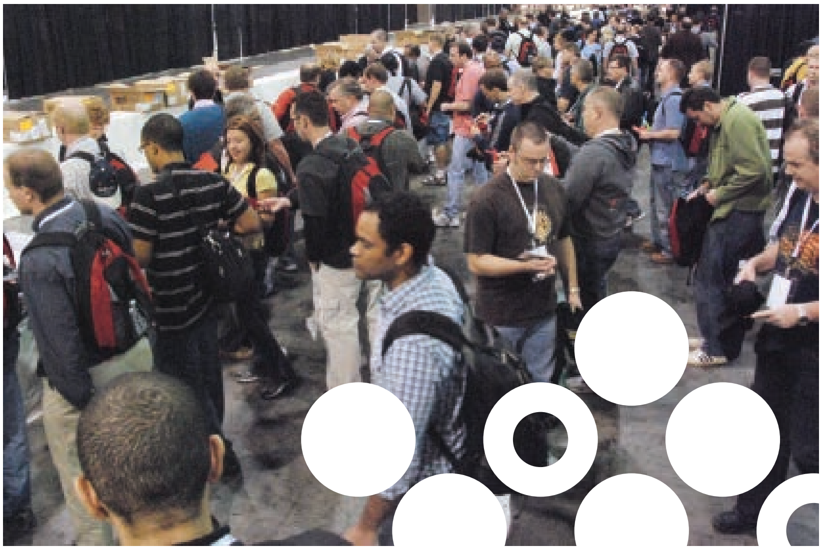
CRUISE GIVEAWAY

Enter to **WIN!**

Enter the contest in the Expo Hall to

WIN a 1 week Caribbean Cruise for two!

You must be Present in the Expo Hall at the time of the drawing to win.



ACTIVE DIRECTORY

MICROSOFT'S GLOBAL FOUNDATION SERVICES AD INFRASTRUCTURE
SEAN DEUBY

When you use Hotmail, or Online Services, or Windows Live, have you ever wondered what kind of infrastructure supports such a wide array of software services? Active Directory, of course. Microsoft's Global Foundation Services group supports these diverse customers. Come to this session to learn more about the GFS computing infrastructure and where it's headed.

AN AD SECURITY REVIEW
SEAN DEUBY

When money is tight, security requirements can still loosen the purse strings. Compare your installation with these Active Directory security best practices, from the well-known to the not-so-obvious. We will also cover Windows 2008 security enhancements; remember, just one capability that really meets your company's business needs can justify the Windows 2008 upgrade and all its other benefits.

WHAT KEEPS IT PROS AWAKE AT NIGHT? AN AD FUNDAMENTALS CHECKLIST
SEAN DEUBY

As an IT professional in a time of shrinking budgets, the top of your to-do list probably involves fighting fires and getting only the most important "must-do" items finished. Your AD is running, but you haven't had time to knock out those important-but-not-urgent AD configuration tasks. Do you have backups that really work? If they do, what about a tested disaster recovery plan that uses them? Do you have a backup copy of your DNS configuration? Attend this session to review what you've done so far, and time-efficient ways to make your AD implementations more secure, reliable, and low effort.

SYSTEM CONFIGURATION & MANAGEMENT

GROUP POLICY: THE NEW HOPE– VISTA AND THE GP PREFERENCES
JEREMY MOSKOWITZ

When was the last time you got a gift? How about 25 gifts? With Microsoft releasing Windows Server 2008, Windows Vista, an updated GPMC, and the Group Policy Preference Extensions, it's like Hanukkah, Christmas and Kwanzaa in one. So learn what every admin needs to know in the new world. Learn why you need a modern management station to support the new GPMC. Learn how to lock out hardware, zap printers, and keep yourself out of trouble with new "MLGPOs." See the 21 new "big things" Microsoft has gifted to every administrator. Even if you're not ready for Windows Vista now, that's okay, you positively must come to this session to learn the ropes from Jeremy Moskowitz, Group Policy MVP. (Note some material is covered in Jeremy's pre-conference workshop.)

THE SCARY TRUTH ABOUT GROUP POLICY
DARREN MAR-ELIA

This session is a highly advanced look at the internals of Group Policy—how it works at the lowest levels and how you can bend it to your will. This session is not for the faint of heart. We will look deep under the covers of Group Policy storage and Group Policy processing, and uncover mysteries such as why some registry policies tattoo and others don't, why Group Policy sometimes seems to work and sometimes doesn't, and other important secrets that Microsoft won't tell you.

TIPS AND TOOLS FOR RAPIDLY DEPLOYING SOFTWARE IN A SMALL ENVIRONMENT
GREG SHIELDS

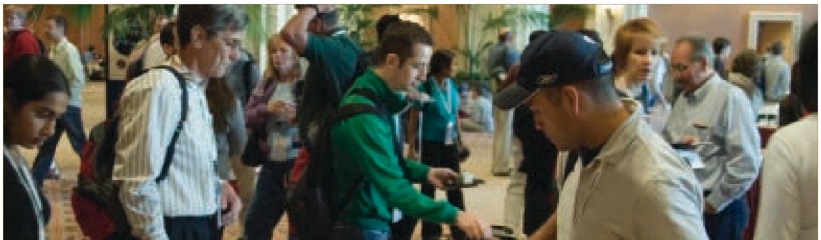
For a lot of small or medium-sized IT environments, the simple act of deploying applications is an operational nightmare. Deploying a single instance of an app takes little more than "Next, Next, Finish". But doing so over dozens or hundreds of computers requires dozens or hundreds of the exact same mouse clicks. In this session, master packager Greg Shields guides you through the skills and the tools to automate all of this. Learn to rapidly package software and deploy it out to any number of computers using no- and low-cost tools. No matter whether you're deploying 5 copies or 500, the skills you'll learn here will ensure every software deployment is a snap.

GETTING USERS TO APPLICATIONS WITH SERVER 2008'S TERMINAL SERVICES
GREG SHIELDS

Terminal Services may well be one of the biggest reasons why you move to Server 2008. Its new capabilities for deploying applications, its new Web interface, its much improved printing, and its new security features all make Terminal Services a real winner. Join Server 2008 expert Greg Shields on a journey through all the new features. You'll see the new TS RemoteApps in action, learn how to deploy Terminal Services apps directly to your user's desktops, and in the end wonder why you haven't upgraded already.

MDOP: SIX AWESOME TOOLS YOU'RE NOT USING TODAY
JEREMY MOSKOWITZ

If you can't handle demos, then don't come to this demonstration. Because it's full of them. In the short time provided, Jeremy Moskowitz, GP MVP, will demonstrate all five tools in Microsoft's popular MDOP (Microsoft Desktop Optimization Pack.) You'll learn how to bring systems back from the dead, prevent applications from killing one another, learn which applications are crashing the most, and how to do some Group Policy magic. If you've already bought MDOP and want to see where all the power lies, or you're just thinking about it, you positively need to come to this session.



CONNECTIONS PARTY

March 17th, 2009

BBQ & CASINO GAMES

Subject to weather conditions.

ENTERPRISE SECURITY MANAGEMENT

SECURING TODAY'S WINDOWS SYSTEMS

MARK MINASI

Server 2008 and Vista share the same basic foundation, which centers around a complete re-write of the Windows kernel. That rewrite came from a Microsoft determined not to repeat the embarrassments of Code Red, Nimda, SQL Slammer, MS Blaster and the rest of our nasty friends. Both Microsoft's desktop and server OSes now tout more secure bases–but are they? In this session, security consultant and writer of Administering Windows Vista Security: The Big Surprises offers a quick and independent overview of Windows security fundamentals and how Vista/Server 2008 Windows' new security tools change the game. Come to this session for some pleasant surprises, and a few chuckles.

NAP YOUR WORLD: HOW TO KEEP YOUR NETWORK FROM CATCHING THE FLU

JEREMY MOSKOWITZ

Cough cough. That's the sound your network makes when one user doesn't "bundle up" with antivirus software. Yep, just one user later, and you've got a big problem. So, how do you contain your little problems so they don't become BIG problems? NAP: Network Access Protection. The idea is that you can quarantine "bad" machines, remediate them and make them "good." While they're "bad" they get limited access and can't hurt others. When they're "good" they get all the network access they need. NAP is nothing to sneeze at. So come by and check it out; so you don't catch the flu.

CREATING A SECURE DESKTOP WITH GROUP POLICY

DARREN MAR-ELIA

This session focuses on practical guidance for using the myriad of security features within Group Policy to create a secure desktop configuration. We will walk through how you can implement features such as Software Restriction Policy, Windows Firewall, IPSec, IE security and related technologies, and provide practical advice that you can implement in your environment right away.

WINDOWS SERVER & CLIENT

FAILED SYSVOL REPLICATION CAN WREAK HAVOC IN YOUR NETWORK

RHONDA LAYFIELD

You spent all that time plugging your security settings into group policies (GPs) and then...the GP fails to replicate to all DCs. Some workstations get the GPs and some don't. Join Rhonda Layfield, a 27-year veteran in the IT industry, to understand the underlying replication engine responsible for ensuring all DCs have consistent GPs. That engine is called the File Replication Service (FRS) and in the past we had no choice–GPs were replicated via the FRS. But Server 2008 introduces a new replication engine–the first ever to make SYSVOL replication more reliable, scalable and manageable–it's called the Distributed File System Replication (DFS-R). In this session, you'll get a complete understanding of FRS, DFS-R and how to migrate your environment from FRS to DFS-R for SYSVOL replication. Don't miss this session if Group Policy replication is important to you.

EASING MANAGEMENT AND SECURING REMOTE OFFICES WITH WINDOWS SERVER 2008

JOHN SAVILL

This session will focus on the technologies in Windows Server 2008 to help ease management of remote offices that require infrastructure but typically don't have local administrators or facilities for proper server storage while increasing security for the organization.

Technologies that will be focused on and demonstrated will include Server Core running ADDS in Read-Only Domain Controller mode with BitLocker encryption. Demonstrations will include services designed to remotely manage a Server Core including winRM, how to automate server core deployment and what exactly a RODC means and a walk-through of configuring which passwords are kept locally on the server with a password hacking tool execution showing most user accounts are not stored negating many of the problems of having unsecured domain controllers out in remote offices.

ADMINISTRATORS' IDOL: THE COOLEST SESSION EVER

DAN HOLME

OK, the title got your attention at least, right? So here's the scoop. From his work with thousands of IT professionals, from the CIOs of Fortune companies to front-line support professionals at the Olympic games with NBC, Dan has amassed a wealth of tricks to boost your productivity as an administrator.

In this fast-paced session, Dan will share how to build truly amazing administrative toolsets that extend your reach, automate tedious tasks, and enable your entire IT organization to work smarter, faster, and more securely. You'll learn tricks that will amaze not only your friends and coworkers, but yourself as well.

Typically part of a post-conference workshop, we've brought this gem into the main event as a fantastic way to cap off your Windows Connections experience. Don't miss it!

SERVER CORE: DO YOU CARE?

DON JONES

Does Windows Server 2008's Server Core matter to you? Should it? Microsoft MVP Don Jones introduces you to Server Core, explains what it can do, shows you how to configure it, how to manage it, and how to maintain it, and–most importantly–helps you understand where it fits in your organization. Learn what Server Core CAN'T do, and what hurdles you may need to overcome if you decide to deploy this new, smaller Windows in your environment.

TIPS YOU ABSOLUTELY MUST KNOW FOR PREVENTING AN ACTIVE DIRECTORY FAILURE

GREG SHIELDS

Is your Active Directory configuration a ticking time bomb? Ever wondered if there's something just not right that could cause a major disaster? Prevent that Resume-Producing Event by attending this fast-paced session. We'll go over the overlooked settings in your AD that could someday cause a major failure. Gleaned from real-world experience through countless AD assessments, you'll learn the top Active Directory mistakes and how to make them right before that bad day arrives.

SHAREPOINT

FILE SHARES AND SHAREPOINT: AN IT SERVICE CRITICAL ANALYSIS

JOEL OLESON

Does you company still have file shares? Is your CIO telling you to get rid of those file servers, but don't put junk into SharePoint? This session will take both a technical and business angle to help you understand and analyze the difficult and often dreaded file-share-to-SharePoint migration question.

21ST CENTURY FILE SHARING: CONFIGURING AND MANAGING DOCUMENT LIBRARIES

DAN HOLME

Many organizations are replacing traditional file shares with SharePoint document libraries, which provide advanced collaborative features. The creation of a document library is simple enough–what comes after that, though, is more nuanced. Join SharePoint MVP Dan Holme for an in-depth examination of document library functionality and configuration. Learn what it takes to make the most of document libraries for 21st century collaboration. This session goes beyond the basics to uncover solutions including:

- The management of end-user shortcuts to frequently used libraries
- Publishing custom templates for new documents in a library
- Configuring and managing document metadata (columns)
- Exposing and inserting SharePoint metadata within Office documents
- Delegating the Override Check Out permission.

- Views versus folders
- Tips for effective e-mail alerts

PERFECT THE ART OF SHAREPOINT SEARCH

WENDY HENRY

Don't let your SharePoint users drift away simply because they cannot find what they're looking for. Hedge your bet by employing the latest SharePoint Search strategies including pre-populated results pages, Best Bet results, RSS feeds of Search result pages and more! Attend this session for live demonstrations of advanced Search administration that will enhance your users' Search experience. Make sure users get to the right information quickly and easily by employing the full range of SharePoint Search tools!

A CLOSE LOOK INSIDE THE SHAREPOINT ENGINE

RANDY WILLIAMS

SharePoint is built on a number of different products and technologies. This session will give you solid architectural overview of both the product and its IIS, SQL Server and .NET Framework foundations. We'll cover IIS Web sites, application pools, configuration and content databases, integration with Active Directory, code access security, and understanding key configuration settings in web.config. And if that isn't enough, we'll also unravel the mystery of how Web site virtualization and redirection actually works.

FITTING SHAREPOINT INTO YOUR ORGANIZATION'S DISASTER RECOVERY PLANS

RANDY WILLIAMS

As more content gets stored in SharePoint, its importance to the organization grows. Is SharePoint part of your Disaster Recovery Plan? If it should be, and you're not sure where to start, this is the session for you. We'll cover numerous scenarios and make sure you have the tools and techniques to recover your data. Out-of-the-box capabilities and third-party solutions will be covered.

INHERITING SHAREPOINT

WENDY HENRY

Anyone who has been handed the keys to an existing SharePoint site or implementation knows that getting information about current structure, layouts and content is difficult at best. Don't let inaccurate or missing information about the environment put your management skills behind the eight ball! Join this session for live demonstrations of tools that will help you investigate and diagram an existing SharePoint implementation. Everyone from new administrators to seasoned consultants will benefit from learning the utilities that make investigating, planning, documenting and auditing SharePoint a breeze!

PRESCRIPTIVE PLANNING AND DESIGN FOR GLOBAL SHAREPOINT DEPLOYMENTS

JOEL OLESON

Do you use one big farm or three medium-sized ones? Whether it's business requirements or technical requirements, we'll break down the global deployment challenges and arm you with the right tools and information for you to be successful.

BASIC DEVELOPER KNOWLEDGE THAT EVERY SHAREPOINT ADMIN MUST HAVE

RANDY WILLIAMS

You may have heard that SharePoint is both a development platform and a product. Its flexibility, while great for developers, can cause administrator heartburn as they try to manage what is becoming a mission critical application. This session will cover many of the must-know concepts such as features, solutions, site definitions and SharePoint scripting. We'll also dive a bit deeper into the underpinnings such as IIS, and the global assembly cache. This session will provide key knowledge that administrators must have to effectively manage a SharePoint environment and be able to communicate with a development team.

SUPPORTING SHAREPOINT DATABASES IN SQL SERVER 2008

WENDY HENRY

Protect your SharePoint investment by protecting the storage facility underneath: SQL Server! This session offers live demonstrations of monitoring and maintenance Best Practices for SQL Server 2008 specific to SharePoint databases. Got a small to medium SharePoint implementation? Learn how to wrangle the Windows Internal Database that installed quietly during your SharePoint installation procedure. Dealing with Enterprise-sized SharePoint? Dive into SQL Server 2008 features that extend and secure your SharePoint databases. Don't let your SharePoint go down with a sinking SQL ship...learn how to best maintain SQL Server and keep SharePoint afloat!

OS AND APPLICATION DEPLOYMENT

WINDOWS DEPLOYMENT SERVICE (MICROSOFT'S NEW RIS): WHY IT'S WORTH THE LOOK!

RHONDA LAYFIELD

Microsoft's new deployment tools ROCK and they're free! If you remember Microsoft's first attempt at a deployment tool–Remote Installation Service (RIS), you might be tempted to overlook the new RIS or Windows Deployment Service or WDS–BUT DON'T. WDS is more user friendly, flexible and powerful than RIS ever dreamed of being. There is now a user interface and configuration settings that will affect deployment methods and your network. One of the biggest complaints in getting started with WDS is "there is too much documentation" you don't know where to start. Join Rhonda Layfield who is one of seven Deployment MVPs in the U.S. and who has been working with WDS for almost two years. She will share her crib notes with you to get you up and running in no time! When you leave this session you will be armed with knowledge, understanding and step-by-step guides so you can get WDS configured, automated, multicast transmissions created and monitored and know how to troubleshoot WDS the day you get back to work.

CREATE YOUR OWN UNATTEND ANSWER FILES FOR VISTA AND SERVER 2008 USING WINDOWS SYSTEM IMAGE MANAGER (WSIM)

RHONDA LAYFIELD

In the past we used Microsoft's Setup Manager to create automated unattended answer files for deploying XP and Server 2003. But there is a new tool in town and it is awesome. It's called Windows System Image Manager and is more robust than Setup Manager ever dreamed of being. But there is a learning curve to it. If you have ever launched this tool and couldn't figure out where to start, let Rhonda Layfield, who is one of 17 Deployment MVPs in the world, show you how to quickly and easily create automated unattended answer files that can be used to install Vista or Server 2008 from DVD or an image stored on a WDS server. Learn about configuration passes: what they are and how you can make them work for you. Lots of demos and step-by-steps to get you started immediately.

VIRTUALIZATION

HYPER-V, WITHOUT THE HYPE: PERSPECTIVE AND PERFORMANCE

MARK MINASI

Microsoft says that Windows Server's Hyper-V Server offers an enterprise-level base for virtual servers... but does it? In this entertaining, cut-to-the-chase look at Hyper-V, industry veteran Mark Minasi (who built HIS first virtual machine on an IBM mainframe running VM in 1982) explains how a few technological changes coupled with some clever ideas led Microsoft to release a virtual machine manager for just $28. What can (and can't) Hyper-V do? What does it do and how does it do it? What operating systems can it run, and which can't it? Join Mark to learn how a grudge match between AMD and Intel made it all possible... and how you'll benefit.

VIRTUALIZATION, THE MICROSOFT WAY

JOHN SAVILL

In this session we will look at all the technologies to facilitate virtualization in your organization and the technical and business benefits. Key technologies explored deal with server virtualization using Hyper-

V (including Clustering Hyper-V), presentation virtualization using new Windows Server 2008 terminal services capabilities, application virtualization using Softgrid and Kidaro technologies. We will look at putting all these technologies together for a Virtual Desktop Infrastructure (VDI) and how solutions such as the Microsoft Assessment and Planning Toolkit help us get a grasp on the benefits virtualization can bring to our organizations.

ESX AND HYPER-V COMPARISON

ALAN SUGANO

Microsoft's own hypervisor, Hyper-V, was released with Windows Server 2008. It is designed to complete directly against VMware's ESX server. How do the two products compare? We'll consider price, performance, hardware requirements, high availability, management and other features in the comparison shootout. If you're evaluating virtualization platforms, make sure to attend this session to assist in your decision making process.

ALL ABOUT MICROSOFT APP-V (SOFTGRID)

JEREMY MOSKOWITZ

Microsoft's made a big investment in "application virtualization." Are you? What was once known as SoftGrid is now known as Microsoft Application Virtualization, or App-V for short. And it's here to solve a big problem. It prevents application conflicts and ends DLL hell. It streamlines application deployment and enables a whole new way of managing applications. It works by "wrapping up" your existing software into "sequences," and then putting them into a virtual sandbox. The upshot? Your applications aren't running "on" Windows. They're running within the sandbox. So, no more desktop deterioration. Oh, and learn how to use your existing management tool (like Group Policy, LANDesk, or SCCM 2007) to deploy SoftGrid applications to your existing desktops and servers. App-V is a big place, but come to this session to make sure you know the ins and outs before you get it in your organization!

NETWORK & STORAGE INFRASTRUCTURE

EVERYTHING YOU WANTED TO KNOW ABOUT STORAGE, BUT WERE AFRAID TO ASK

ALAN SUGANO

If you're like most companies, you are probably running low on disk space as storage-hungry applications eat up disk space like contestants in a pie eating contest. But what's the best solution for your company? With the advent of newer drive interface technologies like Serial Attached SCSI (SAS) and Serial ATA (SATA) there is a lot more to choose from when selecting a storage solution. This session will cover the storage basics of locally attached storage, network attached storage (NAS), just a bunch of disks (JBODs) and storage area networks (SANs), what they are, where they are typically used, and how they fit into a comprehensive storage strategy for your company. We'll also look at the enhancements to Windows Storage Server (WSS) that are scheduled to be released with Windows Server 2008.

SQL SERVER FOR RELUCTANT WINDOWS ADMINS

DON JONES

Are you "Jack of All Tech" in your organization? Are you forced to deal with one or more SQL Server installations that support custom apps or other business needs? Let Don Jones, a self-professed "JoAT" himself, show you JUST what you need to know about SQL Server administration to be effective—without changing your job title to DBA. Learn how SQL Server works, how to install it and keep it patched, where its security vulnerabilities lie, how to perform basic backup and restore operations, how to move a database to a new server, and other key tasks.

BRINGING CLUSTERING TO THE MASSES WITH WINDOWS SERVER 2008

JOHN SAVILL

Windows Server 2008 made great technical improvements to Failover Clustering in Windows Server 2008. Enhancements included new SCSI-3 storage communication removing the hated "SCSI Bus reset", a brand new quorum model removing dependence on components that could be a single point of failure and most of all an interface that makes validating an infrastructure for cluster support, deploying a cluster, and managing a cluster a far more intuitive experience. The end result is to finally bring clustering as a viable option for mortals to use and manage. This session will look at the ways clustering can be deployed including new IP and geographically dispersed options, supported configurations via the new validation tool and the death of the cluster hardware certification, supported storage, aka RIP parallel SCSI, quorum options including witness disk and file share witness and most of all the improved interface allowing administrators to concentrate on making services and applications highly available and less about the underlying cluster structure.

IPV6 FOR THE RELUCTANT: WHAT TO KNOW BEFORE YOU TURN OFF V6 (AND WHY IT MIGHT GET YOU FIRED)

MARK MINASI

Vista has arrived. Windows Server 2008 has arrived. And with them they bring...IPv6. Your first reaction when you see an IPv6 address like "fe80::5efe:10.50.50.112" might be: "Hmmm... that's a lotta colons, and I KNOW what comes out of colons!" But is that the RIGHT reaction? Join veteran Windows explainer Mark Minasi in a look at the latest version of IPv6... and whether you'll want to leave it on or turn it off. In this whirlwind tour, Mark explains the motivation for IPv6 and the technologies behind its implementation (which saves you from having to read 30 RFCs), and then focuses on the specifics of the Microsoft in-the-box IPv6 stack. In the process you may just decide that IPv6 is pretty nifty, after all!

IT MANAGEMENT CONNECTIONS

IT CRYSTAL BALL: IT STRATEGY, ROADMAP AND MICROSOFT DIRECTIONS

PANEL: DAN HOLME, ALAN SUGANO, DON JONES

Join a panel of industry gurus including Dan Holme, Don Jones and Alan Sugano for a detailed look at trends, directions, and Microsoft's technology roadmap. Discover how to align these technologies to support your IT strategies, and buid a blueprint for IT initiatives that save money, reduce waste, increase productivity, and deliver business value. The session will explore Windows 7, Windows Server 2008, Windows Vista, Office and SharePoint 2007 and 2010, as well as server, desktop and application virtualization.

RISKY BUSINESS: WHAT YOU'RE NOT DOING WITH ACTIVE DIRECTORY CAN HURT YOU

PANEL: DAN HOLME, OTHER PANELISTS TBA

Active Directory is a fundamental component of any Windows enterprise, and yet few organizations are implementing Active Directory in ways that deliver real business value. Join Active Directory consultant Dan Holme, along with experts including Jeremy Moskowitz, Darren Mar-Elia and Greg Shields, for a frank discussion of gaps in Active Directory, in the administrative toolsets, in security models, and in process. Learn how to lead your organization to a more secure, compliant, automated, consistent and value-laden implementation of Active Directory. Whether you want to "lock down" administration, streamline configuration, improve asset management, or facilitate compliance auditing, this session will set you up for success.

WHAT DOES COMPLIANCE MEAN TO YOU?

PANEL: DON JONES, OTHER PANELISTS TBA

HIPAA, SOX, GLB, PCI DSS–pick an acronym from today's batch of industry and regulatory requirements and you've got "compliance." But what does all the legal language mean to an IT pro? What exactly do you need to do to your environment to "be compliant?" Can Windows help you do it–or are you going to run across missing features and capabilities? Don Jones, author of numerous books and papers on IT compliance, frankly addresses these questions, guiding you through the commonalities of the major compliance requirements and explaining what Windows out-of-the-box can–and can't–do for you, and what capabilities you'll need to add to become (and remain) truly compliant

WHAT KEEPS CIOS AWAKE AT NIGHT?

PANEL: PANELISTS TBA

Ever wonder what keeps other IT executives up at night, or makes them awaken in a cold sweat? Our industry experts don their "counselor" hats and facilitate a group therapy session for execs. More than "Kumbaya" and group hugs, this is an opportunity to share your concerns and discover what your peers are doing to address them.

ACHIEVING SYSTEMS MANAGEMENT EXCELLENCE IN HETEROGENEOUS DATA CENTERS

PANEL: DARREN MAR-ELIA, OTHER PANELISTS TBA

In this session, we'll focus on technologies and techniques for better managing Windows and Linux server systems in data center environments. We'll look at technologies for cross-platform automation, configuration management and monitoring and examine systems management standards that are facilitating heterogeneous management. We'll also examine third-party products that enhance heterogeneous systems management.

WHAT THE OWNERS MANUAL WON'T TELL YOU... WHY DO SHAREPOINT DEPLOYMENTS FAIL AND WHAT IS GOVERNANCE?

PANEL: JOEL OLESON, OTHER PANELISTS TBA

The SharePoint TechNet planning guides are over 1000 printed pages and there are hundreds of blogs with often conflicting ideas. Why do SharePoint deployments fail? What are the things you MUST do to have a successful deployment? This session will explore failed deployments to help you architect SharePoint Governance and solutions with the true building blocks for success.

SOFTWARE AS A SERVICE/HOSTED APPLICATIONS (OUTSOURCING)

PANEL: ALAN SUGANO, OTHER PANELISTS TBA

Hosted applications is a trend that has a lot of IT Pros worried or at least concerned. With even Microsoft getting into the Software as a Service (SaaS) model, will everyone end up working for the computing cloud in the sky? Are our jobs coming to end as we know it? This session will discuss the advantages and disadvantages of SaaS. In some respects SaaS may be a blessing in disguise allowing IT Pros to focus on more strategic efforts that can really make a difference in a company's success.

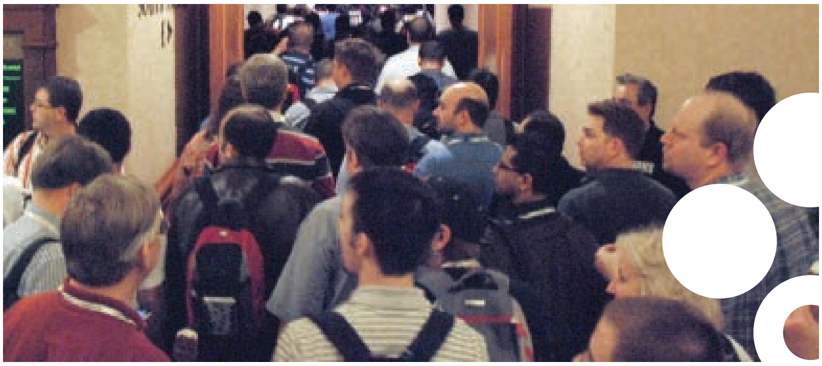
We'll examine how companies fit SaaS into their corporate structure, and how SaaS may or may not fit into your company' strategic IT plans. Is there really a cost savings with SaaS? We'll discuss tips on how to get the best results from SaaS and investigate other possible ways of using SaaS for disaster recovery, testing and high availability.

EVERY ATTENDEE RECEIVES

- Three Lunches
- Three Continental Breakfasts
- Reception
- Connections Party
- Proceedings Resource CD
- Conference T-Shirt and Bag

...and more

SESSIONS PRESENTED BY MICROSOFT



EXCHANGE SERVER 2007 CAS\HUB DEPLOYMENT, SCALING AND TESTING
MICROSOFT

EXCHANGE SERVER 2007 SP1 AND HYPER-V
MICROSOFT

MIGRATING TO EXCHANGE SERVER 2007
MICROSOFT

ADVANCED TROUBLESHOOTING STRATEGIES FOR EXCHANGE SERVER 2007
MICROSOFT

HIGH AVAILABILITY IN EXCHANGE 2007 SP1 - PART 1 - CONTINUOUS REPLICATION AND FAILOVER CLUSTERS
MICROSOFT

HIGH AVAILABILITY IN EXCHANGE 2007 SP1 - PART 2 - DISASTER RECOVERY AND SITE RESILIENCE
MICROSOFT

WHO NEEDS A GUI FOR EXCHANGE? SCRIPT IT!
MICROSOFT

USING EXCHANGE SERVER 2007 FOR VOICEMAIL (AND INTEGRATION WITH OCS 2007)
MICROSOFT

WHAT'S NEW IN OCS 2007 R2?
MICROSOFT

WHAT'S NEW IN CONFERENCING WITH OCS 2007 R2?
MICROSOFT

WHAT'S NEW IN MOBILITY AND WEB ACCESS WITH OCS 2007 R2?
MICROSOFT

PLANNING AND DEPLOYING GROUP CHAT WITH OCS 2007 R2
MICROSOFT

Please Visit Web site for Microsoft Day Session Abstracts!

SPEAKERS AND SESSIONS ARE SUBJECT TO CHANGE. PLEASE SEE WEB SITE FOR UPDATES. WWW.WINCONNECTIONS.COM

DEPLOYING EXCHANGE 2007 WITH WINDOWS 2008 HYPER-V
RICHARD CHRISTOPHER

We'll walk through the options available and ability to consolidate Exchange 2007 deployments using Microsoft Windows 2008 virtualization technology. This session will look at the Exchange roles and deployment scenarios that are 'best fit' for virtualization and consolidation. Elements of an Exchange 2007 Hyper-V design will include the requirements around High Availability and Disaster Recovery and also any impact to performance and service degradation.

TRANSITIONING TO EXCHANGE 2007 USING THIRD-PARTY PRODUCTS
RICHARD CHRISTOPHER

This will cover inter-org-type deployments, where customers wish to transition directly either from legacy Exchange 5.5 to Exchange 2007 or from Exchange 2000/2003 to Exchange 2007. The session will look at the Quest and Priasoft tools to manage the transition and coexistence to Exchange 2007 and highlight any pitfalls and risks during the migration.

COMPLIANCE IN EXCHANGE
KIERAN MCCORRY

This session will cover compliance features in Microsoft Exchange. Check online for a more detailed description closer to the date of the conference.

SNEAK PREVIEW OF EXCHANGE
KIERAN MCCORRY

By the time Exchange Connections Spring 2009 rolls around, Microsoft may have started talking about some of the new functionality available in the next version of Exchange. We'll talk about some of that functionality here. Check online for a more detailed description closer to the date of the conference.

EXCHANGE 2007 UNIFIED MESSAGING PLANNING AND BEST PRACTICES
KARL ROBINSON

This session discusses the inner workings of the Unified Messaging role and the best practices for deployment including the details of performance testing and analysis.

EXCHANGE SERVER 2007 STORAGE SOLUTIONS
KARL ROBINSON

The Exchange Server 2007 mailbox role can be deployed successfully on a variety of storage platforms ranging from Fibre Channel or iSCSI SANs to direct attached storage (DAS) deployments. Serial Attached SCSI (SAS) and small form factor (SFF) disk technology have added to the options available for Exchange storage solutions. This session discusses a range of storage solutions to meet your business needs.

EXCHANGE 2007 SP1 SIZING AND PERFORMANCE: NAVIGATING THE 64-BIT WATERS
STEVE TRAMACK

To achieve the design goals associated with Exchange 2007, many of which were hampered architecturally by Exchange 2003's 32-bit glass ceiling, the move to an x64 architecture was necessary. This session delves into the specific areas of performance and scalability improvement associated with Exchange 2007, addresses new considerations in planning and sizing the various roles and features (including the various replication schemes), and addresses the impact of specific hardware technologies on an Exchange deployment.

HOW TO CONSOLIDATE OVER A QUARTER OF A MILLION MAILBOXES WITH EXCHANGE 2007
MIKE IRELAND

Hear about real-life experiences in consolidating with Exchange 2007 and how such an exercise can better prepare you for future mergers and acquisitions.

OCS 2007 R2 FROM POWERPOINT TO REALITY
DENNIS LUNDTOFT THOMSEN

So you have seen all the nice presentations and demos from Microsoft on Unified Communications and bought the idea!? As you probably guessed, it usually is a tad more complex than the marketing slides try to convince you of, so in this session I will give you the tricks for implementing OCS 2007 R2 in your organization successfully. After this session you will know where to focus your attention before, during, and after your deployment project, including advice on where to focus your attention in terms of the organizational implementation.

WHAT DOES IT TAKE TO VOICE-ENABLE YOUR OCS 2007 R2 DEPLOYMENT?
DENNIS LUNDTOFT THOMSEN

How do you provide OCS 2007 R2 and Exchange with its own voice? This session will focus on all the voice capabilities of OCS and Exchange. We'll discuss the possible scenarios and how to enable them in your environment. This will include detailed discussions on the actual capabilities of the different solutions and based on experience from real-life deployment the efforts required to implement and maintain the different voice scenarios ranging from a pure standalone Enterprise Voice scenario to a full PBX and UM integrated dual forking scenario.

TIPS AND TRICKS FOR MAXIMIZING YOUR INVESTMENT IN UNIFIED COMMUNICATIONS
DENNIS LUNDTOFT THOMSEN

So you have OCS 2007 R2 and/or Exchange 2007 implemented in your organization and you are starting to realize your investment by using presence, click-to-dial, one Unified Messaging inbox etc., but maybe you want even more ROI on your investment? In this session we will do a lap around the platform and look under the hood for developers. We will look at and demonstrate how to integrate business processes with Exchange 2007 SP1 Web services, how to build services that manage communications, and also take a look at Windows Workflows that talk and IM.

WHEN PERFORMANCE IS A PROBLEM, IT'S GOOD TO HAVE A PAL AROUND
WILLIAM LEFKOVICS

Not every company can or wants to deploy SCOM (formerly MOM) to manage and monitor their server deployments. Windows comes with a basic tool called, or at least known as, Performance Monitor. Exchange 2007 Server adds a plethora of perfmon counters for each role. Our PAL, Microsoft's free Performance Analyzer tool, will help us create charts (in HTML–managers love charts) for management and monitoring from perfmon logs of key Exchange counters. We will walk through the requirements (Office Web components, Log Parser, Codeplex) and configuration (XML config files) to produce a simple monitoring solution.

EXCHANGE SERVER 2007 SECURITY BEST PRACTICES
WILLIAM LEFKOVICS

Is Exchange 2007 really secure out of the box? Not necessarily. We will look at all the steps you should take to secure a default installation of Exchange 2007 and what tools are available to confirm or enforce that configuration, specific to each role. We will discuss Microsoft Update, anti-spam updates, the Best Practices Analyzer, and the Security Configuration Wizard (Exchange templates). We'll give consideration to IIS and Windows, including the Microsoft Baseline Security Analyzer (MBSA). We'll discuss anti-virus, anti-malware, anti-spam and Auntie Em.

CONFERENCE SESSIONS

TOOLS, TOOLS, TOOLS! NO, NOT USERS. THE EXCHANGE 2007 MANAGEMENT TOOLBOX

WILLIAM LEFKOVICS

The Exchange Management Console in Exchange 2007 has a section dedicated to tools. It seems, Exchange Server itself needs a little help once and a while. We will review the tools in the EMC covering what they do, when to use them and even when not to. This overview includes: Best Practices Analyzer, Mail Flow TroubleShooter, Queue Viewer, Message Tracking, Database TroubleShooter.

EXCHANGE MESSAGING RECORDS MANAGEMENT

MICHAEL B. SMITH

In this session we will discuss how to use the MRM features of Exchange 2007 to provide the features that were present in Exchange 2003 Mailbox Manager for the deletion of old e-mail. We will be using the Default Folders capabilities so that an Exchange Standard CAL is sufficient.

EXCHANGE HIGH-AVAILABILITY WITH WINDOWS LOAD BALANCING SERVICES

MICHAEL B. SMITH

With all the new features available for HA with mailbox servers (CCR, SCR, LCR, etc.) many people overlook the HA features present for HT and CAS. In this session we will discuss how to provide HA services for CAS, HT, and CAS/HT servers, using both the built-in features of Exchange Server 2007 and WLBS.

EXCHANGE 2007 MONITORING WITH OPSMGR 2007

MICHAEL B. SMITH

Exchange 2007 does not stand alone. It is an application that depends on other infrastructure for it to work properly including Active Directory, DNS, Windows Server, etc. In this session, we will discuss configuring monitoring and health for all facets of an Exchange eco-system, basing health and monitoring on OpsMgr 2007.

TURBO-CHARGED MISSION CRITICAL EXCHANGE DESIGN & ARCHITECTURE

FRANK WRUBEL AND
MARC SUGARMAN

In this session, we will discuss work that has been done to test the limits of Microsoft Exchange Server 2007 using various consolidation methodologies and virtualization technologies, with a particular emphasis on bottom line results/savings. The objective of this effort has been to increase the utilization of large-scale, enterprise-class e-mail environment assets and to reduce the cost to organizations while increasing the security, resilience, and responsiveness to changing end-user and organizational needs. Detailed architectures and best practices will be reviewed.

More Sessions Coming Later ...

We hope to offer a series of sessions by our expert speakers about other topics related to the main subject matter of this conference, but we cannot discuss the details now.

Visit the conference Web site right before the show when we hope to make this information available.

SPEAKERS AND SESSIONS ARE SUBJECT TO CHANGE. PLEASE SEE WEB SITE FOR UPDATES. WWW.WINCONNECTIONS.COM

DATA CENTER BEST PRACTICES
MICROSOFT

See website for abstract.

VIRTUALIZATION—CONSOLIDATE SERVERS, REDUCE ENERGY
MICROSOFT

See website for abstract.

UNIFIED COMMUNICATIONS—REDUCE TRAVEL, INCREASE PRODUCTIVITY, REDUCE EMISSIONS
MICROSOFT

See website for abstract.

MS IT SHOWCASE—WHAT MICROSOFT IS DOING IN IT TO REDUCE THEIR ENVIRONMENTAL FOOTPRINT
MICROSOFT

See website for abstract.

WHAT GREEN MEANS TO IT PROFESSIONALS AND WHY YOU SHOULD CARE
KATHY MALONE

According to Environmental Protection Agency (EPA) guidelines, the highest form of pollution prevention is to not create it in the first place (it is not, as one might think, to manage it well). Similarly, architects and developers are the ones who can optimize their solutions to reduce both the CPU used and the number of bits and bytes sent to the data center, which are two of the main factors determining the size of the data center and the amount of energy used for local processing. So while it is useful for the data center to operate as efficiently as possible, activities conducted by architects and developers have an equally important role to play in Green. This session covers the 7 challenges for architects and developers (patterns). You'll learn how to start collecting business cases and the metrics for Green IT along with solutions that address Green challenges.

GREEN ACROSS THE SUPPLY CHAIN: A GLOBAL PERFECT STORM IS BREWING FOR CHEMICALS. WILL YOU RIDE THE WAVE OR BE WASHED AWAY BY IT?
KATHY MALONE

Although transactions ordinarily move smoothly across the electronic supply, data associated with chemicals traveling that same supply chain typically follow a rockier and more manual road. Historically, legally required information was contained in Material Safety Data Sheets (MSDS). However, new global regulations are changing the information suppliers must provide and that must be available to all employees. Just as we have awesome tools to improve this workflow, the requirements are changing. US Department of Homeland Security chemical screening requirements took effect January 2008, which changes the aggregation requirements around chemicals. The Global Harmonization Standard was implemented by Japan in June 2007, and will reach North America around 2010-2012. The European REACH regulations are in the process of being implemented. Timelines are short, and these initiatives may land in the lap of your IT department for immediate implementation if your company produces, distributes or uses any chemicals. This session will prepare you with an overview of the new requirements and how improving the workflow around this activity gives you two times the green: it makes your process more efficient (which is more green), and has you better managing the chemicals in an environmentally responsible manner.

GREENING YOUR BUSINESS CASE AND YOUR CORPORATE CULTURE: USING GREEN TO SUPPORT YOUR PROJECTS
KATHY MALONE

Until Green metrics become part of all IT activities from the gleam in the future user's eye through maintenance activities after successful deployment, and become part of every bid specification and RFQ, the mindset around building Green and Sustainable will not change. Green needs to be an end-to-end consideration in the same way security is built in now. Back in the mid-80's contractors were forced to implement bar-coding and chemical tracking during construction of an automotive assembly plant by including it as a requirement in the bid specification. Similarly, including the requirements for Green metrics as part of the procurement process will cause all bidders to address the question, and start building the knowledge base around these activities. In-house, review of processes from a Green prospective early in the design activity may soon be required of us. Within manufacturing and other industry segments, this consideration is already required to some extent for chemicals. You'll learn about the tools available and how to use them to best manage these activities to introduce Green responsibility in your organization.

GREENHOUSE GAS FOOTPRINTING
CAROL DOLLARD

Five greenhouse gases are organized into three scopes and a standardized calculation based primarily on the scientific makeup of these chemicals. The resulting number is often called the "carbon footprint". Learn how to calculate the carbon footprint, particularly the carbon footprint of your IT organization. You may have heard of carbon offsets. Learn what this accounting agreement means and more about the upcoming legislation regarding carbon credits and offsetting. You'll leave this session with an understanding of what your carbon footprint means and how to reduce it.

ENERGY OF IT
CAROL DOLLARD

IT runs on equipment that runs on energy. Take a quick look back at the energy shifts of moving from mainframes to today's networks and look forward to the impact of energy on your organization's bottom line. Explore energy efficiency and options for reducing your overall energy consumption. You'll see how to calculate energy payback to ensure you consider energy lifecycle costs as you make IT investments. Even if you aren't able to make significant hardware changes to improve efficiency, you can reduce your energy costs through conservation and you'll get materials to help you publicize energy efficiency such as differences between Sleep, Hibernate and Off and the impact of various energy settings to reduce the individual energy load of each piece of your infrastructure.

E-WASTE AND LIFECYCLE
CAROL DOLLARD

The short lifecycle of IT and consumer electronics creates a significant and growing waste stream. The hardware in your IT infrastructure includes materials that potentially harm the environment-including lead in CRT monitors, mercury in LCD monitors, cadmium in batteries, and bromide-based flame retardants. Your organization has long-term legal responsibility for your waste stream and in the US, two sets of federal regulations apply. Get an overview of these regulations, understand why some items in your infrastructure meet the legal description of a hazardous waste and learn what accounting you need on these components as you dispose of them. You'll also learn a little about an ugly side of recycling where a significant portion of the recycling stream is shipped overseas. You'll leave this session with a better understanding of your e-waste stream and how to reduce it.

TELECOMMUTING
CAROL DOLLARD

Workers in your organization spend an amazing amount of time in their vehicles. Based on data in the 2000 census, the average commute nationwide is 25 minutes, or nearly 500 hours per year. Add to that the massive environmental and quality-of-life issues associated with commutes and telecommuting becomes an attractive alternative. In many cases, it also allows you to hire expertise that is not available within commuting distance. So, if telecommuting is so great, why aren't we all doing it? This session looks at some of the challenges and benefits of telecommuting for information workers and developers. It will include an open floor segment so you can hear the successes and failures of other organization and hone in on the types of workers you want to remotely support.

DevConnections

MICROSOFT ASP.NET CONNECTIONS · VISUAL STUDIO & .NET CONNECTIONS · SQL SERVER CONNECTIONS · SharePoint CONNECTIONS

MARCH 22-25, 2009

ORLANDO, FL • JW MARRIOTT & THE RITZ CARLTON

The cutting-edge event for developers and DBAs

Register by Jan 12th and receive a FREE night at JW Marriott. (based on a 3-night minimum stay)

>> *The first 500 people to register will be mailed SQL Server 2008 standard with one CAL*

CHECK WEBSITE FOR DESCRIPTIONS OF SESSIONS AND WORKSHOPS

www.DevConnections.com

800.438.6720 • 203.268.3204

DevConnections

Where a passion for technology has no boundaries!

- 80+ MICROSOFT AND INDUSTRY EXPERTS
- 150+ IN-DEPTH SESSIONS
- UNPARALLELED WORKSHOPS
- EXCITING ANNOUNCEMENTS

New

- UNSTRUCTURED/INTERACTIVE EVENING SESSIONS

Technology+Solutions=Impact

Connect to Microsoft architects and industry experts to separate technology myths from reality!

Scott Guthrie
Microsoft
Corporate Vice President, .NET Developer Division

Thomas Rizzo
Microsoft
Director, SharePoint Group

Dave Mendlen
Microsoft
Director of Developer Marketing

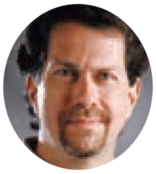
Microsoft · msdn magazine · SQL Server magazine · Dr.Dobb's · TECH Conferences Inc. PENTON MEDIA

A SAMPLING OF SPEAKERS & MICROSOFT EXPERTS

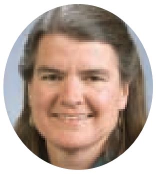
SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND BIOS.

FRANCOIS AJENSTAT
MICROSOFT

LEE BENJAMIN



SEAN DEUBY
ADVAIYA INC.



CAROL DOLLARD
COLORADO STATE UNIVERSITY

RICHARD CHRISTOPHER
HP

THOMAS FOREMAN
WADEWARE

DAN HOLME
INTELLIEM
WINDOWS CONNECTIONS CONFERENCE CHAIRPERSON

MIKE IRELAND
HP

DON JONES
CONCENTRATED TECHNOLOGY

RUSS KAUFMANN
MINDSHARP

RHONDA LAYFIELD
CONSULTANT/TRAINER

WILLIAM LEFKOVICS
MOJAVE MEDIA GROUP, LLC

DENNIS LUNDTOFT THOMSEN

JOEL OLESON

KATHY MALONE
MANGUARD SYSTEMS, INC.

DARREN MAR-ELIA
SDM SOFTWARE, INC.

KIERAN MCCORRY
HP
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR

MARK MINASI
MR&D

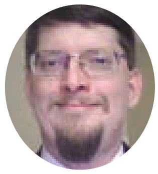
JEREMY MOSKOWITZ
MOSKOWITZ, INC.

STEVE RILEY
MICROSOFT

PAUL ROBICHAUX
3 SHARP,
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR

JOHN SAVILL
EMC

GREG SHIELDS
CONCENTRATED TECHNOLOGY



MICHAEL B. SMITH
HP

ALAN SUGANO
ADS CONSULTING

MARC SUGARMAN
UNISYS

STEVE TRAMACK
HP

RANDY WILLIAMS
SYNERGY CORPORATE TECHNOLOGIE

FRANK WRUBEL
UNISYS

ADDITIONAL SPEAKERS INCLUDE:

WENDY HENRY SHAREPOINT-ELEARNING.COM · **KARL ROBINSON**

... And many more

The cost of a workshop is in addition to the regular conference fee.

PRE-CONFERENCE WORKSHOPS

SATURDAY, MARCH 14

FULL DAY PRE-PRE-CONFERENCE • 9:00AM-4:00PM

EXTREME ADMINISTRATIVE MAKEOVER: BUILDING A MORE PERFECT ENTERPRISE

DAN HOLME

Increase security. Improve manageability. Ensure compliance. Lower risk. Oh, and do it all with half the budget of last year. Does this sound like your mandate? Then this full-day preconference workshop is for you! Join one of the industry's leading Microsoft technologies consultants, Dan Holme, for a deep dive into solutions that address common IT administration pain points. Learn to streamline, automate, and secure your adminsitrative practices and tricks to improve the administration and configuration of users, computers, and Active Directory as a whole. Solutions in this session include:

- Implementing least privilege for Active Directory administration: advanced administrative delegation.
- Assigning computers to users, tracking user logon and computer location.
- Role-based access control and role-based management: ensuring security and audit trail.
- Tricks to improve application deployment, regardless of your deployment and management tools.
- Managing user data and settings: beyond profiles and redirected folders.

FULL DAY PRE-PRE-CONFERENCE • 9:00AM-4:00PM

TRANSITIONING TO EXCHANGE SERVER 2007 WORKSHOP: THE UPGRADE PATH IS CLEAR. ***Bring your own laptop.***

LEE BENJAMIN

While Exchange Server 2003 is a great email platform, Exchange Server 2007 is better and it's time to upgrade. Spend a day listening to lecture and working through labs that transition an Exchange Server 2003 organization to Exchange Server 2007. With a new architecture and many new features, the process of implementing Exchange Server 2007 must be carefully planned and executed. In this workshop you will get valuable guidance and best practices for transitioning to Exchange 2007 as well as hands-on experience.

NOTE: The laptop you bring MUST have at least 2GB of memory, 20GB free disk space, and dual layer DVD drive.

SUNDAY, MARCH 15

FULL DAY PRE-CONFERENCE • 9:00AM-4:00PM

SHAREPOINT JUMP START: REIMAGINING COLLABORATION

DAN HOLME

If you are new to SharePoint, or are trying to wrap your head around the massive potential of this powerful platform, you'll be the hero of your enterprise when you bring back the solutions you discover in this fast-paced, full-day preconference workshop. Dan Holme, a Microsoft MVP for SharePoint, will dive deep into the configuration, customization, and management of SharePoint collaboration. You'll learn to build SharePoint solutions that address common enterprise challenges, and you'll be amazed just how much you can do with Windows SharePoint Services (WSS) without having to pay for Microsoft Office SharePoint Server (MOSS). Topics include:

- SharePoint Administration Jump-Start: What you need to know to administer SharePoint effectively, in 90 minutes or less.
- How to use SharePoint document libraries as a replacement for traditional file shares.
- Driving effective collaboration and end-user adoption with Microsoft Office 2007 applications as SharePoint clients.
- How to build "Business Intelligence Lite", no-code, and low-code SharePoint solutions using Office 2007 and SharePoint Designer.

FULL DAY PRE-CONFERENCE • 9:00AM-4:00PM

MAKING EXCHANGE SERVER 2007 HIGHLY AVAILABLE

RUSS KAUFMANN

This all day session will cover the installation and configuration of failover clustering. This session will cover:

- Using Single Copy Clustering as well as Clustered Continuous Replication clusters.
- How to use Network Load Balancing for Client Access Services and Hub Transport.
- Multiple sites and providing disaster recovery for Exchange.

Attendees will leave with a strong understanding of how High Availaiblity can be implemented for an Exchange Server 2007 environment and how to explain the benefits and costs associated with the different options available. Here's a quick rundown of the order of topics presented:

Outline of Modules:

- Installing/Configuring Failover Clustering
- Configuring Single Copy Clusters (SCC)
- Configuring Clustered Continuous Replication (CCR)
- Multiple Location Solutions, including Standby Continuous Replication (SCR)
- Configuring Network Load Balancing (NLB)
- Configuring NLB for Client Access Services and Hub Transport for client relays

FULL DAY PRE-CONFERENCE • 9:00AM-4:00PM

WALK IN THE PARK: MICROSOFT EXCHANGE 2007 HANDS-ON LABS ***Bring your own laptop.***

LEE BENJAMIN

Come take a six-hour guided tour of Exchange Server 2007 and see for yourself the next evolution of the world's most powerful messaging system. Experience the new Management Console, the five new server roles, e-mail policy enforcement and compliance, powerful new scripting tools, new architecture, new high availability and disaster recovery features, new mailbox features, and methods for migrating from earlier versions of Exchange. In this information-packed day with Exchange expert and MVP Lee Benjamin, you'll get hands-on experience with Exchange Server 2007 using your laptop to walk through several labs developed by Wadeware®.

NOTE: The laptop you bring MUST have at least 2GB of memory, 15GB free disk space, and DVD drive.

HALF-DAY MORNING PRE-CONFERENCE • 9:00AM-12:00PM

GROUP POLICY FUNDAMENTALS, SECURITY, AND CONTROL

JEREMY MOSKOWITZ

Group Policy is the most efficient way to manage desktops in a Windows environment. If you are still running to machines to install and configure desktops, you are not taking full advantage of the power of Group Policy. In this practical workshop, Jeremy Moskowitz will help you gain control of your environment and get your life back. This is the perfect workshop to take before doing "deep dives" into the main sessions of the conference. You'll get a little bit of everything: deployment, configuration, control, and security! We'll warm up with some Group Policy basics. Then, you'll learn how to get your XP and Vista client machines up and running with some new set-up options. After your machines are up and running, Jeremy will show you how to manage your environment with GPOs. You'll get some "solid base hits" to ensure you can go back to work with some good ideas you can immediately put to use. For instance, learn how to zap printers down to your computers, and remotely deploy software to your users' desktops, and learn how to use Group Policy to secure collections of machines. You'll also get a sneak-peek at the Group Policy Preferences, the newest Microsoft technology that's 100% free—and it will get you out of login-script hell. We'll examine how Group Policy can do the heavy lifting to the jobs you want to do! This session has both XP and Vista content.

NOTE: Some material is repeated in Jeremy's regular sessions as reinforcement.

HALF-DAY AFTERNOON PRE-CONFERENCE • 1:00PM-4:00PM

VIRTUALIZATION: A REAL-WORLD JUMP START

ALAN SUGANO

Virtualization is one of the hot topics this year. With significant increases in performance of the current generation of server hardware with quad-core processors, high memory capacity, and Serial Attached SCSI (SAS) drives, much of the processing power on a server goes unused. Virtualization allows you to take advantage of this processing power by running several virtualized servers on one physical host. If you're considering virtualization and are new to this technology, this workshop will get you up to speed. You'll learn about the following topics:

- Virtualization hardware. Server processors, memory and hard drive configurations. Optimization of the hardware and the virtual environment for the best virtual guest performance. Running the x64 platform for virtual hosts and guests.
- Virtualization software (Virtual Server 2005, VMware Server, ESX Server).
- Backup strategies of virtual servers.
- Virtualization and high availability. Learn about the high availability solutions from Microsoft and VMware in the virtual server environment.
- Virtual guest limitations and how to determine if virtualization is a good fit for your application.

POST-CONFERENCE WORKSHOPS

THURSDAY, MARCH 19

FULL DAY POST-CONFERENCE • 9:00AM-4:00PM

WINDOWS POWERSHELL CRASH COURSE

DON JONES

Want to start taking advantage of Microsoft's new management shell, but don't know where to start? Start here, with the industry's most-recognized and experienced PowerShell instructor, Don Jones! Co-author of Windows PowerShell: TFM and more than 30 other IT books, Don's easygoing and popular teaching style will help you understand what PowerShell is all about, how to start using the shell immediately (no scripting required), and how to automate complex business processes using PowerShell's simplified scripting language. With a focus on real-world examples (and lots of take-home code), you'll soon be brimming with ideas for automating tedious administrative processes. This is not a hands-on workshop; no laptop is required and power is not provided. No prior scripting or PowerShell experience is necessary—and this will be the ONLY full-day PowerShell workshop Don offers on the East Coast in 2009!

FULL DAY POST-CONFERENCE • 9:00AM-4:00PM

WALK IN THE PARK: OFFICE COMMUNICATIONS SERVER HANDS ON LABS *Bring your own laptop.*

THOMAS FOREMAN

Come take a six-hour guided tour of Office Communications Server (OCS) 2007 and see for yourself the latest Microsoft Unified Communications product. Much, much more than Instant Messaging, Office Communications Server provides text, web conferencing, and Voice over IP solutions that allow you to change the way your organization communicates. We will also review the new features of OCS 2007 R2. We'll install and configure OCS 2007, as well as Office Communicator 2007 and the Live Meeting 2007 client and how to configure and use Communicator Web Access. In this information-packed day, you'll use your laptop to walk through several hands-on labs developed by Wadeware® with OCS expert, Thomas Foreman.

NOTE: The laptop you bring MUST have at least 4 GB of memory, 30 GB free disk space and a dual layer DVD drive, optional and a webcam and headset with microphone is recommended

HOTEL INFORMATION

HOTEL ACCOMMODATIONS

The Hyatt Regency Grand Cypress Resort, One Grand Cypress Blvd., Orlando, FL is the conference site and host hotel. SPACE IS LIMITED so reserve your room early by calling the conference hotline at 800-505-1201.

AIRLINE

Please call Pericas Travel at 203-562-6668 for airline reservations.

CAR RENTAL

Hertz is offering auto rental discounts to attendees. Call the Hertz Meeting Desk at 800-654-2240 for reservations and refer to code CV# 010R0037 to receive your attendee discount.

AIRPORT SHUTTLE

Mears Transportation is the designated ground carrier at Orlando International Airport. You may pick up the shuttle on Level 1, one floor below baggage claim. The shuttle is available 24 hours a day. The rates to the Hyatt Regency Grand Cypress hotel are as follows: One-way is $20.00 and $33.00 round-trip. You may call Mears directly at 407-843-2404 for more information or go to their Web site: www.mearstransportation.com. Prices are subject to change.

ATTIRE

The recommended dress for the conference is casual and comfortable. Please bring along a sweater or jacket, as the ballrooms can get cool with the hotel's air conditioning.

ORLANDO, FLORIDA

EXTEND YOUR STAY

Come early or stay late. Bring the family! You are in the land of fantasy for children of all ages. Walt Disney World - Magic Kingdom® Park, Disney MGM Studios®, Epcot® and Disney's Animal Kingdom® Theme Park. In addition, explore Kennedy Space Center, Sea World, and Universal Studios Theme Park, or take a short drive to beautiful white sand Atlantic beaches.

TAX DEDUCTION

Your attendance to a WinConnections conference may be tax deductible. Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

SPONSORSHIP/EXHIBIT INFORMATION

For sponsorship information, contact: Rod Dunlap
phone: 480-917-3527
e-mail: rod@devconnections.com
See web site for more details. www.WinConnections.com

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

Call 800-505-1201 to take advantage of group discount pricing.

1-3 registrants	$1,495 per person
Additional registrants after the 3rd (4th, 5th, 6th...)	$1,295 per person ($200 off each)

NOTES & POLICIES: The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our Web site at www.WinConnections.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague. Please inform us if you have any special needs or dietary restrictions when you register. The conference registration includes a one-year print subscription to *Windows IT Pro*. Current subscribers will have an additional 12 issues added to their subscription. Subscriptions outside of the United States and Canada will be digital. $25 of the funds will be allocated toward a subscription to *Windows IT Pro* ($49.95 value). **REGISTRATION & CANCELLATION POLICY:** Registrations are not confirmed until payment is received. Cancellations before February 3, 2009 must be received in writing and will be refunded minus a $100 processing fee. After February 3, 2009 cancellations and no shows are liable for full registration, it can be transferred to the next Connections Conference within 12 months or to another person. Active Directory, Microsoft, MSDN, Outlook, Windows Server, Windows Vista, and Windows are either trademarks or registered trademarks of Microsoft Corporation. All other trademarks are property of their owners.

CONFERENCE REGISTRATION • MARCH 15-18, 2009

FULL CONFERENCE REGISTRATION INCLUDES KEYNOTE ON MARCH 15, 6:30PM,
THROUGH CLOSING SESSION MARCH 18, 4:30PM

ONLINE
www.WinConnections.com
E-MAIL
info@devconnections.com
PHONE
(800) 505-1201, (203) 268-3204
FAX
(203) 261-3884
MAIL
Microsoft Exchange Connections 2009
Windows Connections 2009
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

NAME ____________ PRIORITY CODE ____________

COMPANY ____________ TITLE ____________

STREET ADDRESS (REQUIRED TO SHIP MATERIALS) ____________

CITY, STATE, POSTAL CODE ____________ COUNTRY ____________

TELEPHONE ____________ FAX ____________ E-MAIL ADDRESS (IMPORTANT) ____________

❑ **Microsoft Exchange Connections** .... on or before February 3rd .... $1395.00 ____________
.... after February 3rd .... $1495.00 ____________

❑ **Windows Connections** .... on or before February 3rd .... $1395.00 ____________
.... after February 3rd .... $1495.00 ____________

PRE-CONFERENCE WORKSHOPS

SATURDAY, MARCH 14, 2009 — LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

❑ 9:00AM - 4:00PM Extreme Administrative Makeover: Building a More Perfect Enterprise HOLME .... $399 ____________
❑ 9:00AM - 4:00PM Transitioning to Exchange Server 2007 Workshop ... BRING YOUR OWN LAPTOP BENJAMIN .... $399 ____________

PRE-CONFERENCE WORKSHOPS

SUNDAY, MARCH 15, 2009 — LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

❑ 9:00AM - 4:00PM SharePoint Jump Start: Reimagining Collaboration HOLME .... $399 ____________
❑ 9:00AM - 4:00PM Making Exchange Server 2007 Highly Available KAUFMANN .... $399 ____________
❑ 9:00AM - 4:00PM Walk in the Park: Microsoft Exchange 2007 Hands-on Labs BRING YOUR OWN LAPTOP BENJAMIN .... $399 ____________
❑ 9:00AM - 12:00PM Group Policy Fundamentals, Security, and Control MOSKOWITZ .... $199 ____________
❑ 1:00PM - 4:00PM Virtualization: A Real-World Jump Start SUGANO .... $199 ____________

POST-CONFERENCE WORKSHOPS

THURSDAY, MARCH 19, 2009 — LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

❑ 9:00AM - 4:00PM Windows PowerShell Crash Course JONES .... $399 ____________
❑ 9:00AM - 4:00PM Walk in the Park: Office Communications Server Hands On Labs BRING YOUR OWN LAPTOP FOREMAN $399 ____________

CONFERENCE MATERIALS

Full conference registration includes materials for the one conference for which you register.
You may purchase materials for the other concurrently run events.

❑ Microsoft Exchange Connections Proceedings CD .... $75 ____________
❑ Windows Connections Proceedings CD .... $75 ____________

PAYMENT — TOTAL ____________

*IMPORTANT: You must reference Microsoft Exchange Connections or Windows Connections on your check.

❑ CHECK (payable to Tech Conferences) All payments must be in US Currency. Checks must be drawn on a US bank.

❑ VISA ❑ MASTERCARD ❑ AMEX

CREDIT CARD NO. ____________ EXPIRATION DATE ____________

Cardholder's Signature ____________ Cardholder's Name (print) ____________

WinConnections

MICROSOFT EXCHANGE CONNECTIONS

UNIFIED COMMUNICATIONS CONNECTIONS

WINDOWS CONNECTIONS

IT MANAGEMENT CONNECTIONS

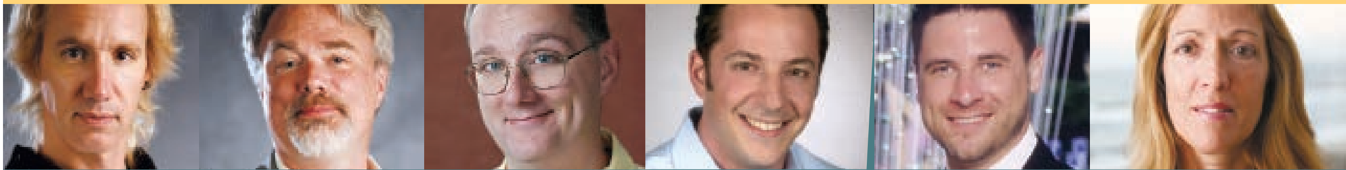
GREEN IT CONNECTIONS

BONUS: SharePoint Administration for IT Pros Track

MARCH 15-18, 2009 • ORLANDO, FL • Hyatt Regency Grand Cypress

REGISTER TODAY • www.WinConnections.com

800.505.1201 • 203.268.3204



STEVE RILEY	MARK MINASI	PAUL ROBICHAUX	FRANCOIS AJENSTAT	DON JONES	RHONDA LAYFIELD
MICROSOFT	MR&D	3SHARP	MICROSOFT	CONCENTRATED TECHNOLOGY	CONSULTANT/ TRAINER

WinConnections 2009
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

TRACK ACTIVE DIRECTORY CHANGES

Use this handy script for do-it-yourself AD auditing

by Jim Turner

ILLUSTRATION BY BRUNO MALLART / IMAGES.COM

Where I work, we have a relatively large domain and Active Directory (AD) changes daily: Users are added or moved from one organizational unit (OU) to another, admins leave the company and new ones join—you get the picture. Tracking all those changes manually would be virtually impossible for one person, but with the help of the AccountTracker.vbs script, it's almost effortless.

AccountTracker.vbs captures a snapshot of specific AD objects such as groups and members of groups and writes the distinguished name (DN) of each object along with a run date and category to an .xml file in the form of an ActiveX Data Objects (ADO) database. (If you're not familiar with ADO, read "Rem: Obtaining Data from a SQL Server Database," InstantDoc ID 25628, and "Introduction to ADO," InstantDoc ID 98718.) Each subsequent run of the script compares the new database with the previous database. By using a simple compare process, you can detect new AD objects as well as objects that existed in the previous database but aren't present in the new database.

As you'll see, I structured this script to query specific groups, but you can add your own queries within the code fairly easily and start keeping tabs on the objects of your choice. The script does cover a wide range of AD objects and should provide you with useful and comprehensive reports.

AccountTracker.vbs helps you monitor general AD activity, and, more importantly, it's a valuable tool that you can use to spot new accounts or missing accounts that were added to or removed from security groups such as Enterprise Admins, Domain Admins, and Administrators. With this script you can also see new, moved, disabled, or deleted user and computer accounts, spot OU changes, and keep tabs on group membership changes that take place within groups such as Server Operators and Account Operators.

Querying Sets of AD Categories

The script's main thrust is on querying two sets of AD categories. The first set pertains to groups and class queries that can ascertain AD objects with fairly generalized LDAP query statements:

- AdminGroups: any group name containing the string Admin
- ComputersDisabled: disabled computer accounts; ComputersEnabled: enabled computer accounts
- Groups: all groups
- GroupsNoMembers: groups that have no members
- OUs: all OUs
- Servers: all computer objects whose operatingSystem attribute value contains the string Server
- ServiceAccounts: any account whose description attribute value contains the string Service
- ServiceGroups: any group whose sAMAccountName attribute value contains the string Service
- UserAccountsDisabled: disabled user accounts

The second set requires a bit more scripting logic than the first set. It centers on obtaining memberships of the following high-level security-related groups:

- Account Operators
- Administrators
- Backup Operators
- Domain Admins
- Enterprise Admins
- Replicator
- Schema Admins
- Server Operators

The script evaluates group membership, which involves checking for nested groups, acquiring members of nested groups if nested groups exist, avoiding endless loop recursion should nested groups refer to each other, and checking for domain accounts whose primary group is set to a group being evaluated. As you are probably aware, if an account's primary group is set to a specific group name, querying that specific group's membership won't return that account nor any other accounts whose primary group is set to that specific group.

How AccountTracker.vbs Works

When the script is run, each object from both sets of category queries is written to an ADO disconnected recordset. Each record contains the script's run date, the object's DN, the category description, and a concatenation of the category and the DN. I'll explain those areas, including the concatenated field, in the next section.

After the script's initial run, all AD changes in any of the defined object categories can be detected on a subsequent run simply by traversing the current run's database and checking it against the previous run's database. The script checks each record in the previous database against the new database to see if the previous object still exists in the new database. If a record from either database isn't found in the other, that record is written to a Microsoft Excel spreadsheet. After all of the records have been written to the spreadsheet, an Excel pivot table worksheet is produced within the Excel workbook showing the AD changes by categories of new AD objects and by objects that weren't found, providing a clear snapshot of changes that took place between the dates of the newest run and the previous run.

How often you run this process should be determined by the amount of activity your domain undergoes. The more activity you have, the more frequently you should run the process. I run mine daily, but if activity should slow down, I can choose to run it only once a week. Incidentally, I have coded the script so that you can easily run it as a scheduled task. I avoided using message boxes created with VBScript's MsgBox function; instead, I used pop-ups created with Windows Script Host's (WSH's) WshShell.Popup method. Message boxes shouldn't be used in scripts that run as scheduled tasks because they don't go away until a user clicks a button. Unlike message boxes, pop-ups appear for only a given number of seconds. The added benefit of pop-ups is that you see the messages even if you decide to run the script manually.

The databases created and used in this script contain the four fields I mentioned earlier: Rundate, which is simply the date that the script was run; Category, which is an item from one of the two sets of categories I described (e.g., UserAccounts-Disabled); DN, which is the DN of the AD object; and CatDN, which is a combination of the values in the Category and DN fields. The reason for concatenating the values in the two fields has to do with the way ADO functions when you use the Find method to find a record within the database.

As much as I like ADO, one of its shortcomings is that you can't use the AND operator with the Find method—and my script depends on finding a category and a DN. An alternative to the Find method, the Filter method, lets you use the AND operator. However, I found that using the Filter method with midsized and larger databases (i.e., those containing more than 500 records) resulted in terrible performance hits on my computer. I decided to take the disk-space hit over the performance hit and combined the two fields so I could use the speedy Find method.

You need to carefully consider where you choose to house your databases. Depending on the size of your domain, you could have databases that are a few megabytes in size for every run of the script. Currently each of my databases is roughly 3.5MB. You can, of course, zip or archive older databases if need be. The .xml files zip quite nicely; a 3.5MB file zips down to approximately 145KB. To change the default storage location, find the line

```
DBPath = C:\Scripts\ADacctTrack\
```

in the script and change *C:\Scripts\ADacctTrack* to the appropriate path.

The first time you run this script, only the XML database is produced because there's nothing to compare it with. Whenever the script is run, the database produced is saved as NewestAcctTracker.xml when the process completes. When you run the script a second time, the previous database is renamed PreviousAcctTracker.xml and the database created from the current run is named NewestAcctTracker.xml. On the third and all subsequent runs, the database named PreviousAcctTracker.xml is renamed ArcAcctTracker*DateTime*.xml (e.g., ArcAcctTracker09-26-20081305-45.xml).

DateTime will always be the DateLastModified property value of PreviousAcctTracker.xml before it's renamed. I obtain this value by using the GetFile method of the Scripting.FileSystemObject object to access the PreviousAcctTracker.xml file properties. I store the value in a variable named DateTime, making sure I fill dates with leading zeroes (e.g., 07/07/2008), convert the time portion of the date to military time (e.g., 1307:54), and replace every slash (/) and colon (:) with a hyphen (-). This naming convention lets you easily find a specific database by date. The files also sort by name more appropriately when you use this naming convention.

One last note about how the script works before we explore the code. When the script runs, it creates a new ADO disconnected recordset. After the script retrieves the data from the category queries and stores it in the ADO database, it opens the previous database, steps through each of the new records in the ADO database, and attempts to find that record within the previous database. If it can't find that data, then that record is considered new because it didn't exist in the previous database, and the record is written to an Excel spreadsheet. Each record written to the spreadsheet includes

- a Status entry of New
- a Category entry that refers to the Category field of the current database record
- a DN entry that refers to the DN field of the current database record
- a Note entry of *Not in Previous List.*

After reaching the end of the file in the current database, the script steps through each record in the previous database and attempts to find a matching record in the current database. If a matching record isn't found, that record is considered "not found" and data from the previous database is written to the spreadsheet. The Status entry in this case becomes Not Found, and the Note entry becomes *In Previous – Not in Most Recent List.*

A Not Found entry could mean that the object in question could have been deleted, moved, renamed, or disabled. Whatever the case, the original DN and category of that entry no longer exist. It's certainly possible that the object in question will appear in one of the other categories as a "New" object, unless the object was deleted. You'll see later on that I sort the master worksheet by DN rather than Status or Category—that sort method makes finding moved, disabled, and renamed objects much easier because the DN entries are grouped together.

Looking at the Code

Since most of the code is relatively straightforward, I concentrate on the areas of main importance rather than doing a detailed section-by-section code analysis. The excerpt in Listing 1, page 28, shows the code that creates the arrays used by AccountTracker .vbs to query the AD categories. Although a good bit of code precedes that in Listing 1, there's nothing that can't be readily understood by reading through the code.

The code at callout A uses the Dim statement to declare the Categories array, which contains 11 elements. The code then assigns values to each element. Be mindful of any modifications you make to this code. If you add or remove any elements, you must adjust the Dim statement to the appropriate number. These elements are going to be the first set of category names that get written to the database along with the accompanying AD objects' DN.

The code in callout B declares the LDAPFilter array, which stores the LDAP query statements for the categories defined in the Categories array. Obviously each query statement must correspond to the appropriate category

Let's take a look at one of the LDAP queries—the one stored in element 0 of the LDAPFilter array. This query is associated with the value stored in element 0 (AdminGroups) of the Categories array. In the LDAP statement, you can see that the query looks for an AD objectCategory attribute value equal to *group* and AD objects that have a sAMAccountName attribute value that contains the string *admin*.

Note how each element in the LDAPFilter array is designed to correspond to an element in the Categories array. It's important that they correspond because the associated category is written to the database for each collection object, as you'll see shortly.

In callout C, I sort the disconnected recordset so that the database is sorted by the CatDN field in ascending order. Next, I start a For...Next statement that steps through each element in the LDAPFilter array and places the element's value into a string that I use to create a collection of AD objects for each category. I construct the LDAP query string in this statement:

```
strQuery = "<LDAP://" & DNC & ">;" _
  & LDAPFilter(i) _
  & ";DistinguishedName;subtree"
```

I then execute the query against AD with these statements:

```
objCommand.CommandText = strQuery
Set objRecordSet = objCommand.Execute
```

Afterward, I simply cycle through the returned recordset and write the collection object information to the ADO database with the lines of code in the Do...Loop statement in callout C. This cycle is repeated for

Listing 1: Code That Creates the Arrays Used to Query the Two Sets of AD Categories

```
Ⓐ Dim Categories(10)
Categories(0) = "AdminGroups"
Categories(1) = "ComputersDisabled"
Categories(2) = "ComputersEnabled"
Categories(3) = "Groups"
Categories(4) = "GroupsNoMembers"
Categories(5) = "OUs"
Categories(6) = "ServersWintel"
Categories(7) = "ServiceAccounts"
Categories(8) = "ServiceGroups"
Categories(9) = "UserAccountsDisabled"
Categories(10) = "UserAccountsEnabled"

Ⓑ Dim LDAPFilter(10)
' Groups whose sAMAccountName attribute value contains the string admin
LDAPFilter(0) = "(&(objectcategory=group)(samaccountname=*admin*))"
' Disabled computer accounts
LDAPFilter(1) = "(&(objectCategory=computer)" _
  &
"(userAccountControl:1.2.840.113556.1.4.803:=2))"
' Computer accounts that aren't disabled
LDAPFilter(2) = "(&(objectCategory=computer)" _
  & "(!userAccountControl:1.2.840.113556.1.4.803:=2))"
' Groups
LDAPFilter(3) = "(objectCategory=group)"
' Groups with no members
LDAPFilter(4) = "(&(objectCategory=group)(!member=*))"
' OUs
LDAPFilter(5) = "(objectCategory=organizationalunit)"
' Just servers
LDAPFilter(6) = "(&(objectCategory=computer)(operatingSystem=*server*))"
' User accounts whose description attribute value contains the string service
LDAPFilter(7) = "(&(objectcategory=user)(description=*service*))"
' Groups whose sAMAccountName attribute value contains the string service
LDAPFilter(8) = "(&(objectcategory=group)(samaccountname=* service*))"
' Disabled user accounts
LDAPFilter(9) = "(&(objectCategory=user)" _
  & "(userAccountControl:1.2.840.113556.1.4.803:=2))"
' User accounts that aren't disabled
LDAPFilter(10) = "(&(objectCategory=user)" _
  & "(!userAccountControl:1.2.840.113556.1.4.803:=2))"

Ⓒ DRS.Sort = "CatDN ASC"
For i = 0 to Ubound(LDAPFilter)
  strQuery = "<LDAP://" & DNC & ">;" & LDAPFilter(i) _
    & ";DistinguishedName;subtree"
  objCommand.CommandText = strQuery
  Set objRecordSet = objCommand.Execute
  Do Until objRecordSet.EOF
    DRS.AddNew
    DRS("RunDate") = Date()
    DRS("Category") = Categories(i)
    DRS("DN") = objRecordSet.Fields("DistinguishedName").Value
    DRS("CatDN") = Categories(i) & _
      objRecordSet.Fields("DistinguishedName").Value
    objRecordSet.MoveNext
  Loop
  Set objRecordSet = nothing
Next

Ⓓ ' Get members of specific groups. Pay particular attention to the DNs.
' You might need to modify them.
' DNQA is an abbreviation for DistinguishedName Query Array.
Dim DNQA(7)
DNQA(0) = "CN=Account Operators,CN=Builtin," & DNC
DNQA(1) = "CN=Administrators,CN=Builtin," & DNC
DNQA(2) = "CN=Backup Operators,CN=Builtin," & DNC
DNQA(3) = "CN=Domain Admins,CN=Builtin," & DNC
DNQA(4) = "CN=Enterprise Admins,CN=Builtin," & DNC
DNQA(5) = "CN=Replicator,CN=Builtin," & DNC
DNQA(6) = "CN=Schema Admins,CN=Builtin," & DNC
DNQA(7) = "CN=Server Operators,CN=Builtin," & DNC

Dim MemberCats(7)
MemberCats(0) = "AccountOperators"
MemberCats(1) = "Administrators"
MemberCats(2) = "BackupOperators"
MemberCats(3) = "DomainAdmins"
MemberCats(4) = "EnterpriseAdmins"
MemberCats(5) = "Replicator"
MemberCats(6) = "SchemaAdmins""
MemberCats(7) = "ServerOperators"
```

each LDAPFilter element.

A similar process takes place for the second set of categories, except that this set collects members of groups. Callout D shows a similar layout of categories and query arrays, and a similar looping process takes place for these arrays' elements. However, the process branches off and calls a subroutine that evaluates each group and writes all the members and their associated categories to the database.

Be sure to check the DNs in the DistinguishedName Query Array (DNQA) for accuracy. You or your domain administrator might have moved some of these groups into another OU. For example, it isn't an uncommon practice to move Domain Admins, Enterprise Admins, and Schema Admins from the Users container into the Builtin container. If AccountTracker.vbs finds that any of these Admins are incorrectly placed, a 15-second pop-up message lets you know which DNQA elements weren't found. If you do have to modify the DN, just change the portion within the double quotes. For example, if your Domain Admins were in the Builtin container rather than the Users container, you'd change

```
DNQA(3) = "CN=Domain Admins,CN=Users," _
  & DNC
```

to

```
DNQA(3) = _
  "CN=Domain Admins,CN=Builtin," _
  & DNC
```

DNC should remain untouched. That's your Domains Default naming context, which needs to be concatenated to the portion of the DN within the quotation marks.

The GetGroupMembers subroutine in Listing 2, page 30, is called for this group of categories. The code at callout A first gets the group's primaryGroupToken attribute value and uses an LDAP query to find accounts that have matching primaryGroupID attribute values. This step usually isn't necessary when performing group membership listings, but it eliminates the possibility of missing members with out-of-the ordinary primary groups defined, which is particularly important for Domain Admin groups.

In callout B, you'll notice that before any item in the returned collection is written, the sAMAccountName attribute value is checked to see whether it exists in a diction-

ITS JOB IS TO HELP MAKE YOURS MORE PRODUCTIVE.

intel® Xeon® inside™
Powerful. Efficient.

IBM System x3350 Express

$1,849

OR $48/ MONTH FOR 36 MONTHS[1]

THE SERVER THAT PRACTICALLY MANAGES ITSELF.

Stop doing those routine tasks that tie you up for hours. IBM System x3350 Express monitors your infrastructure from a single point of control. Proactively identifies potential problems. And helps you solve them quickly. Let System x servers take on more routine tasks, so you can take on more challenges.

From the people and Business Partners of IBM.
It's innovation made easy.

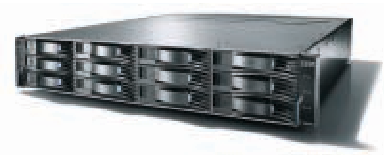
PN: 4193E2U

Featuring Intel® Xeon® Processors X3330 (2.66 GHz/1333 MHz), 6 MB L2 QC, 2x2 GB, open bay SAS 2.5˝ HS

Predictive Failure Analysis and Light Path Diagnostics; redundant, hot-swappable power supplies and fans; and up to 4 hard disk drives

3-year, next business day, on-site limited warranty[2]

IBM has more ways to help you get more done.



IBM SYSTEM STORAGE DS3200 EXPRESS **$4,495** OR $117/ MONTH FOR 36 MONTHS[1]

PN: 172621X

Up to six 3.5˝ SAS or SATA HDDs or up to eight 2.5˝ SAS HDDs and internal tape backup option for storage protection

Integrated RAID capability, -0, -1 and -1.0; RAID-5 optional

Comes with a 3-year on-site limited warranty[2] on parts and labor. 3-year 24x7 on-site repair (PN: 21P2078) with a 4-hour response is available for an additional $600

IBM Express "Bundle and Save"

We bundle our Express systems to give you the accessories you need – while saving you money on the hardware you want. Act now. Available through **ibm.com** and IBM Business Partners.

IBM® express advantage™

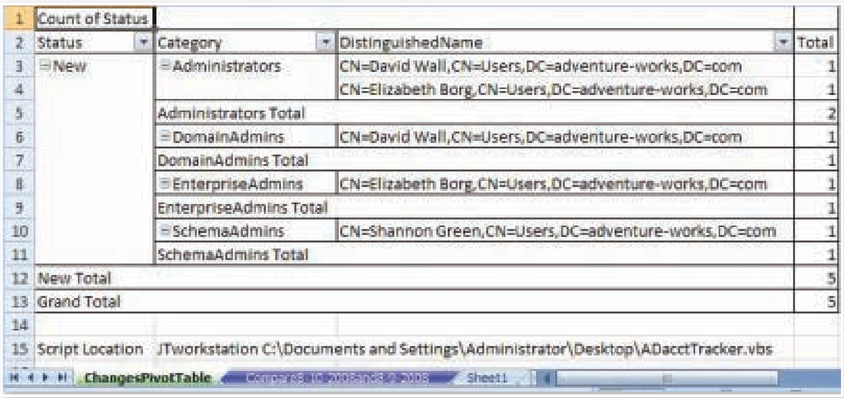
ibm.com/systems/simplifyit
1 866-872-3902 (mention 6N8AH14A)

1. IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.
2. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit: ibm.com/servers/support/machine_warranties or write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services, including those designated as ServerProven® or ClusterProven®. Telephone support may be subject to additional charges. For on-site labor, IBM will attempt to diagnose and resolve the problem remotely before sending a technician. On-site warranty is available only for selected components. Optional same-day service response is available on [select] systems at an additional charge.

Listing 2: The GetGroupMembers Subroutine

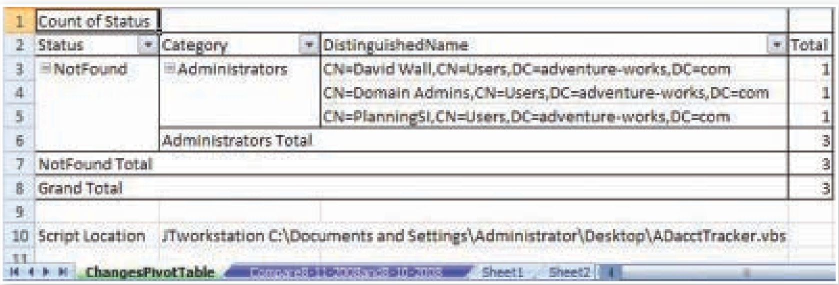
```
Sub GetGroupMembers(Grp)
  Grp.GetInfoEx Array("primaryGroupToken"),Ø
A TokNo = Grp.Get("primaryGroupToken")
  LDAPfiltVar = "(primaryGroupID=" & TokNo & ")"
strQuery = "<LDAP://" & DNC & ">;" & LDAPfiltVar & _
  ";samaccountname,distinguishedname;subtree"
  objCommand.CommandText = strQuery
  Set objRecordset = objCommand.Execute
  Do Until objRecordset.EOF
    sam = objRecordset.Fields("samaccountname").Value
    dname = objRecordset.Fields("distinguishedname").Value
B If Not dictionaryObj.Exists(sam) Then
    dictionaryObj.Add sam,sam
    ' Add category and DN information.
    DRS.AddNew
    DRS("RunDate") = Date()
    DRS("Category") = MemberCats(j)
    DRS("DN") = objRecordSet.Fields("DistinguishedName").Value
    DRS("CatDN") = MemberCats(j) & objRecordSet.Fields
    ("DistinguishedName").Value
  End If
  objRecordset.MoveNext
  Loop
  objRecordset.Close

  For Each memobj In Grp.Members
C   If Not dictionaryObj.Exists(memobj.samaccountname) Then
      dictionaryObj.Add memobj.samaccountname,memobj.samaccountname
      If Lcase(memobj.Class) = "group" Then
        DRS.AddNew
        DRS("RunDate") = Date()
        DRS("Category") = MemberCats(j)
        DRS("DN") = memobj.distinguishedname
        DRS("CatDN") = MemberCats(j) & memobj.distinguishedname
        GetGroupMembers(memobj)
      Else
        ' Add category and DN information.
        DRS.AddNew
        DRS("RunDate") = Date()
        DRS("Category") = MemberCats(j)
        DRS("DN") = memobj.distinguishedname
        DRS("CatDN") = MemberCats(j) & memobj.distinguishedname
      End If
    End If
  Next
  Set memobj = Nothing
  Set objRecordset = Nothing
End Sub
```



1	Count of Status			
2	Status	Category	DistinguishedName	Total
3	New	Administrators	CN=David Wall,CN=Users,DC=adventure-works,DC=com	1
4			CN=Elizabeth Borg,CN=Users,DC=adventure-works,DC=com	1
5		Administrators Total		2
6		DomainAdmins	CN=David Wall,CN=Users,DC=adventure-works,DC=com	1
7		DomainAdmins Total		1
8		EnterpriseAdmins	CN=Elizabeth Borg,CN=Users,DC=adventure-works,DC=com	1
9		EnterpriseAdmins Total		1
10		SchemaAdmins	CN=Shannon Green,CN=Users,DC=adventure-works,DC=com	1
11		SchemaAdmins Total		1
12	New Total			5
13	Grand Total			5
14				
15	Script Location	JTworkstation C:\Documents and Settings\Administrator\Desktop\ADacctTracker.vbs		

Figure 1: Sample pivot table of results after running script



1	Count of Status			
2	Status	Category	DistinguishedName	Total
3	NotFound	Administrators	CN=David Wall,CN=Users,DC=adventure-works,DC=com	1
4			CN=Domain Admins,CN=Users,DC=adventure-works,DC=com	1
5			CN=PlanningSI,CN=Users,DC=adventure-works,DC=com	1
6		Administrators Total		3
7	NotFound Total			3
8	Grand Total			3
9				
10	Script Location	JTworkstation C:\Documents and Settings\Administrator\Desktop\ADacctTracker.vbs		

Figure 2: Sample pivot table of results after deleting Domain Admins group

ary. If it doesn't exist, the object is written to the database and the value is added to the dictionary. You'll also notice that the same type of process is undertaken as with the first set of categories when writing a record to the database. The category element—in this case MemberCats(j)—contains the name of the group currently being evaluated.

After checking the primary group, the process at callout C gets members of the group. The code first checks a dictionary for the existence of the group or member name. If the group or member name exists in the dictionary, it's bypassed and the next member is retrieved from the group member collection. If the member isn't in the dictionary, it's added to the dictionary.

Next, the member item is checked to see if it is a group. If it is, the group item is written to the database and a recursive call is made to the GetGroupMembers subroutine to retrieve members from nested groups. By checking the dictionary for existing group and member names, we can avoid endless loops should nested groups refer to each other. If the member is not a group, the routine simply writes the member data to the database. This process is repeated for each element in the DNQA.

After all categories have been evaluated and written to the database, all that's left to do is compare the newly collected data with the previous data. That process is the same as that used for the Categories array.

Examining the Results

Sometimes I use a little trick to get an Excel report of changes that took place over the entire month. First I move the NewestAcctTracker.xml and PreviousAcctTracker.xml databases to a folder named SafeKeep. Then I copy the ArcAcctTrackerDateTime.xml file that I want to compare to the current run, rename that copy NewestAcctTracker.xml, and run AccountTracker.vbs.

Next, I save my spreadsheet—as Account changes for August.xls, for instance. Then I move the original copies of NewestAcctTracker.xml and PreviousAcctTracker.xml from the SafeKeep folder to their original location and overwrite the existing temporary files.

Let's look at some sample spreadsheets. Say that I start off with members in the group Administrators, which includes Domain Admins and Enterprise Admins. Under

Category	Status	DistinguishedName	Note
UserAccountsEnabled	NotFound	CN=Wilson Brown,CN=Users,DC=adventure-works,DC=com	In Previous - Not in Most Recent List
GroupsNoMembers	NotFound	CN=Server Operators,CN=Builtin,DC=adventure-works,DC=com	In Previous - Not in Most Recent List
Groups	New	CN=NewGroup,CN=Users,DC=adventure-works,DC=com	Not in Previous List
GroupsNoMembers	NotFound	CN=Backup Operators,CN=Builtin,DC=adventure-works,DC=com	In Previous - Not in Most Recent List
DomainAdmins	New	CN=anna,CN=Users,DC=adventure-works,DC=com	Not in Previous List
UserAccountsDisabled	New	CN=anjali,CN=Users,DC=adventure-works,DC=com	Not in Previous List
UserAccountsEnabled	NotFound	CN=anjali,CN=Users,DC=adventure-works,DC=com	In Previous - Not in Most Recent List
ServerOperators	New	CN=Alice Serventi,CN=Users,DC=adventure-works,DC=com	Not in Previous List
BackupOperators	New	CN=Alan Jackson,CN=Users,DC=adventure-works,DC=com	Not in Previous List
GroupsNoMembers	NotFound	CN=Account Operators,CN=Builtin,DC=adventure-works,DC=com	In Previous - Not in Most Recent List
AccountOperators	New	CN=Abigail Gonzalez,CN=Users,DC=adventure-works,DC=com	Not in Previous List

ChangesPivotTable | Compare8-12-2008and8-11-2008 | Sheet1 | Sheet2 | Sheet

Figure 3: Sample spreadsheet of results after making multiple changes

Count of Status

Status	Category	DistinguishedName	Total
New	AccountOperators	CN=Abigail Gonzalez,CN=Users,DC=adventure-works,DC=com	1
	AccountOperators Total		1
	BackupOperators	CN=Alan Jackson,CN=Users,DC=adventure-works,DC=com	1
	BackupOperators Total		1
	DomainAdmins	CN=anna,CN=Users,DC=adventure-works,DC=com	1
	DomainAdmins Total		1
	Groups	CN=NewGroup,CN=Users,DC=adventure-works,DC=com	1
	Groups Total		1
	ServerOperators	CN=Alice Serventi,CN=Users,DC=adventure-works,DC=com	1
	ServerOperators Total		1
	UserAccountsDisabled	CN=anjali,CN=Users,DC=adventure-works,DC=com	1
	UserAccountsDisabled Total		1
New Total			6
NotFound	GroupsNoMembers	CN=Account Operators,CN=Builtin,DC=adventure-works,DC=com	1
		CN=Backup Operators,CN=Builtin,DC=adventure-works,DC=com	1
		CN=Server Operators,CN=Builtin,DC=adventure-works,DC=com	1
	GroupsNoMembers Total		3
	UserAccountsEnabled	CN=anjali,CN=Users,DC=adventure-works,DC=com	1
		CN=Wilson Brown,CN=Users,DC=adventure-works,DC=com	1
	UserAccountsEnabled Total		2
NotFound Total			5
Grand Total			11

Script Location JTworkstation C:\Documents and Settings\Administrator\Desktop\ADacctTracker.vbs

ChangesPivotTable | Sheet1 | Sheet2

Figure 4: Sample pivot table of the results in Figure 3

Domain Admins Properties, Members, I had Administrator and Planning. Under Enterprise Admins Properties, Members, I had Administrator. Under Schema Admins Properties, Members, I had Administrator.

Suppose I then ran the script and added more members. Under Domain Admins Properties, Members, I added David Wall; under Enterprise Admins Properties, Members, I added Elizabeth Borg; and under Schema Admins Properties, Members, I added Shannon Green. Figure 1 shows the resulting Excel pivot table.

Now assume that someone removed the Domain Admins group from the Administrators group. When the script is run again, the resulting pivot table in Figure 2 shows that the Domain Admins group wasn't found. It also reveals that the members of that group are no longer members of the Administrators group; thus their status shows as Not Found. However, those users are still members of the Domain Admins group.

Finally, the spreadsheet in Figure 3 shows what the report would look like if I added an Account Operator, a Backup Operator, a member to the Domain Admins group, a group called NewGroup, and a member to the Server Operators group; disabled an account; and deleted an account. The New section of the pivot table in Figure 4 shows what was added, but you might need to review the Not Found section a little closer to understand what's happened.

Testing and Using the Script

At the TechNet Virtual Lab "Microsoft Office PerformancePoint Server 2007 - Excel Dashboards" (see go.microsoft.com/?linkid=8205426), you can copy the code to the virtual-server sandbox so you don't have to make changes to AD. Paste the code by clicking the Action button. (Check the pasted code for accuracy, as the paste routine chops up code.) I comment out the *On error resume next* statement and run the script until I get no errors.

You can create simple, easy-to-use .xml database files for keeping history-related data. I use these files to monitor my printers as well as keep track of all domain account SIDs, and I reference them when checking the Recycle Bin on servers.

InstantDoc ID 100428

Jim Turner
(jturnervbs@gmail.com) is a domain administrator and applications developer for Computer Sciences Corporation.

Protect SharePoint with ISA Server 2006

Easy load balancing and authentication for your SharePoint farms

by Jim Boyce

Microsoft ISA Server 2006 sports a host of features that extend its capabilities as a front end for SharePoint beyond those of earlier versions and make ISA Server easier to administer in that role. These features provide enhanced load balancing, easier server publishing, better detection for redundancy, and other improvements. In this article, we look at three SharePoint-related topics for ISA Server 2006: load balancing, using wildcard certificates for authenticating multiple sites, and using forms-based authentication.

Load Balancing Web Front-End Servers

Load balancing enables a group of servers in a web farm to service requests for the same content so that the workload is shared across the servers in the farm. Regardless of whether you use a hardware or software solution, load balancing is essential to your web farm topology in two primary ways. First, it distributes the load across the servers in the farm, improving overall performance and providing redundancy. Second, load balancing lets you more easily scale the farm as load on the farm increases. In the case of a SharePoint farm, you simply add another web front-end server to the farm, then add it to the server group in ISA Server, which begins distributing a share of the load to the new server.

ILLUSTRATION BY TODD DAVIDSON / IMAGES.COM

Balancing traffic between web servers is just one requirement, however. To handle load balancing gracefully, the solution must also be able to detect failed or offline servers so that consistent and predictable failover can occur. If the web service hangs on a given server, for example, the load-balancing solution needs to detect that failure and exclude the affected server from the group, transferring the load to the remaining servers in the farm. Such detection isn't a simple matter of a heartbeat or ping between the load balancer and the individual farm servers because the web service could be hung and unresponsive though the server itself still responds to pings.

In addition, when web front-end servers are brought online, they need to be added to the balanced farm without affecting current client connections. So, whether a failed server is brought back online or another server is implemented to replace it, the load-balancing solution needs to integrate the server into the farm's overall workload seamlessly and transparently.

ISA Server treats the web front-end servers in a SharePoint web farm as a single entity. When you set up a web farm in ISA Server, you specify either the IP addresses or host names of the servers in the farm. If you specify host names, ISA Server needs to be able to resolve those names to the IP addresses of the target servers. In addition, you specify the method you want ISA Server to use to monitor server connectivity within the farm. As Figure 1 shows, you can use an HTTP/HTTPS GET request, send a Ping request, or establish a TCP connection to each server; the method you choose applies to all servers in the farm. ISA Server performs a verification check every 30 seconds for each server in the farm, with a default response timeout of 5,000 milliseconds.

Probably the best option for server-health detection for a SharePoint farm is the HTTP/HTTPS GET method because it accommodates situations where the web service has failed on a target server but the server is still responding to pings or is able to create a TCP connection. If the server responds to GET requests, it's a good bet that the server is available and the web service is running.

To use the GET method, you specify a URL that ISA Server will check and prefix the URL with an asterisk (*) to represent the server host name. For example, assume that your farm includes web front-end servers named MOSSWFE01 and MOSSWFE02, and you want to test at the site top level. You specify a URL of http://*/default.aspx for connectivity testing when you set up the farm in ISA Server. When performing the connectivity check for the servers, ISA Server replaces the asterisk with the host names and derives the URLs http://mosswfe01/default.aspx and http://mosswfe02/default.aspx for testing. If your SharePoint configuration requires it, you can specify a custom host header in the URL.

Publishing a SharePoint farm is fairly straightforward thanks to the SharePoint Site Publishing Rule Wizard. Before you run the wizard, however, there are a couple of additional steps to take:

- Determine the communication method between ISA Server and the farm. You can use either HTTP or HTTPS, as applicable to your situation and infrastructure.
- Determine the server farm members, and optionally create the server farm object. The members are the servers that are running the Web Server role in the SharePoint farm. You can create the server farm object prior to running the wizard or you can create it within the wizard.
- Determine the web listener settings. The web listener specifies the ISA Server networks and IP addresses on those networks that will listen for external connection requests, the authentication method and forms to be used, the number of allowed connections, what certificates are used, single sign-on settings, and a handful of other related settings.
- Determine the authentication mechanism that ISA Server uses to authenticate to the web servers. If you're authenticating all your users against Active Directory (AD), NTLM suffices in most situations. However, you can also choose to negotiate Kerberos or NTLM, constrain authentication to Kerberos only, use Basic authentication, or use no delegation. Each method has situations where it's the best choice, so do your planning ahead of time to determine which method fits your farm's requirements.
- Specify alternate access settings. Although you don't need to specify these settings in SharePoint before running the wizard, you'll have to do it at some point before deploying the farm. You configure alternate access mapping in SharePoint Central Administration.

With these decisions behind you and your web servers up and running, you're ready to publish your farm. To launch the wizard, open the ISA Server Management console, right-click the Firewall Policy node, and choose New, SharePoint Site Publishing Rule. After you specify a name for the rule and click Next, the wizard gives you three options, as Figure 2 shows:

- *Publish a single Web site or load balancer*—Use this option to publish a single web server or publish a load-balanced farm that sits behind another load balancer.
- *Publish a server farm of load balanced Web servers*—Use this option to load balance the farm using ISA Server.
- *Publish multiple Web sites*—Use this option to publish multiple websites. The wizard creates a rule for each site.

The second option is the one to use when ISA Server is load balancing the web front-end servers for your SharePoint farm. As you move through the wizard, you'll be asked for responses to the following prompts:

- Internal Publishing Details—Specify the internal site name for the web farm, which is typically the name that users use when accessing the farm internally.
- Specify Server Farm—You can choose an existing farm object or create a new one. If you're creating a new farm, specify the farm object name, the name or IP address of each server in the

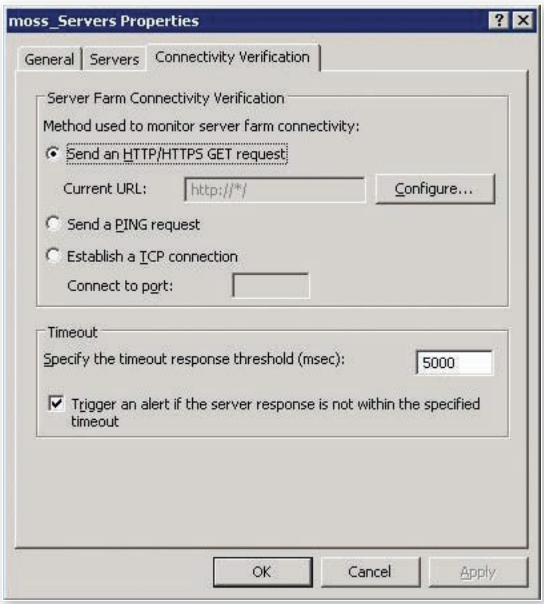


Figure 1: Choosing a method for ISA Server to monitor server connectivity within a farm

farm, and the monitoring method that ISA Server will use to monitor server availability within the farm.

- Public Name Details—Specify whether ISA Server accepts requests for all domains or only for a specific domain. If you're specifying a single domain, you enter the Fully Qualified Domain Name (FQDN) for the farm, such as www.contoso.com.
- Select Web Listener—Select an existing web listener or create a new one on the fly. Regardless of which option you choose, you can edit the listener properties within the wizard or afterward.
- Authentication Delegation—Choose the authentication method that ISA Server will use to authenticate to the web farm.
- Alternate Access Mapping Configuration—Specify whether alternate access mappings are already configured on the SharePoint farm.
- User Sets—Specify how the publishing rule is applied. By default, it's applied to all authenticated users, but you can add, edit, and remove user sets as needed.

To view the rule settings after you create them, open the Firewall Policy node and double-click the rule. You can review and edit settings as needed and also modify the default settings for rules that aren't set through the wizard, such as schedule and link translation.

The properties for the rule also specify how the rule handles client affinity, ensuring that the same web front-end server handles all requests for a particular client. The Web Farm tab lets you choose between cookie-based (session affinity) and source IP–based (IP address affinity). Session affinity provides more reliable client affinity and is recommended for SharePoint farms.

Using Wildcard Certificates

If your SharePoint farm hosts multiple websites, such as www.constoso.com, support.contoso.com, and partners.contoso.com, and you need to secure those sites with SSL, you need to decide whether to use individual SSL certificates or a single wildcard certificate.

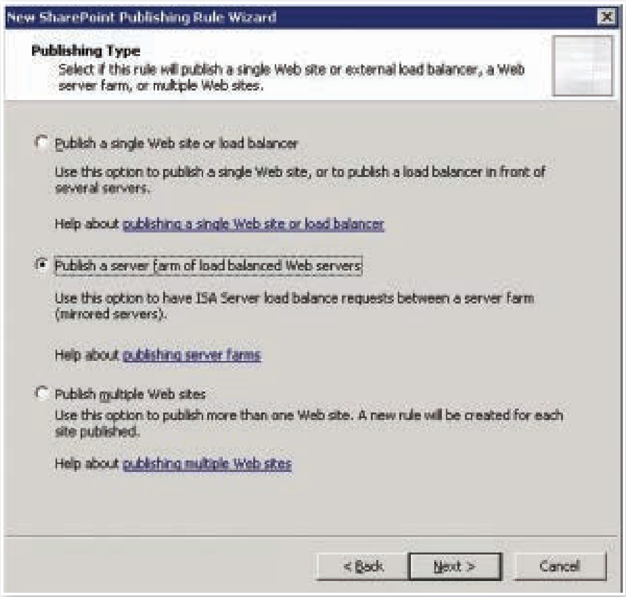


Figure 2: Selecting the publishing type for load balancing in the New SharePoint Publishing Rule Wizard

An SSL certificate includes a common name as one of its properties. The common name must match the host header being submitted by the client's browser, or a certificate error occurs. For example, the common name on a certificate for the site www.contoso.com should be www.contoso.com. If you map support.contoso.com to the same site and users browse to that URL, they'll see a certificate error because the host header, support.contoso.com, doesn't match the common name in the certificate. Depending on how the client browser is configured, users might not be able to browse to the site.

A wildcard certificate lets you use a single certificate for multiple sites in a domain. Instead of a common name that matches the site name, the wildcard certificate uses an asterisk in the common name in place of the host name. So, in this example, the common name of the certificate would be *.contoso.com. Any site in the contoso.com domain can then be served by this single certificate.

Both types of certificate have their advantages. If you're hosting a relatively small number of sites, individual certificates are probably less expensive than a wildcard certificate. As the number of sites increases, you see a tradeoff between ease of administration and cost: It's easier to manage a single certificate and you can deploy as many sites as you need without adding other certificates, but you pay more for that convenience and flexibility.

To determine whether a wildcard certificate is the right solution for you, look at the number of sites you'll be hosting and the cost differential between that number of individual certificates and a single wildcard certificate. For example, if individual, one-year certificates are $995 and a wildcard certificate is $15,995, then your break-even point is essentially at 16 sites; with any more than 16 sites, you'll pay less if you purchase a wildcard certificate. But you should also factor in any projected growth in your number of sites and how much it's worth to you to not have to manage multiple certificates, in order to answer the question of which option is best in your environment.

Note that you aren't limited to using a certificate only on ISA Server. If you want to secure traffic between ISA Server and the web front-end servers for your SharePoint farm, you can also install certificates on the front-end servers. As Figure 3, page 36, shows, when you run the wizard to create the publishing rule, you specify that ISA Server will use SSL to connect to the servers in the published web farm.

To use a wildcard certificate to publish multiple websites with a single web listener, first obtain the wildcard certificate and install it in the machine store on each ISA server in the array. After you install the certificate, create the new web listener that you'll use to publish the sites. In the New Web Listener Definition Wizard, when prompted to select the certificates for the web listener, choose the option *Use a single certificate for this Web Listener*, then choose the wildcard certificate.

Forms-Based Authentication

Forms-based authentication uses HTML forms to authenticate users, and ISA Server 2006 supports forms-based authentication to published SharePoint servers. ISA Server 2006 provides three sets of forms: HTML

for standard browsers, and Compact HTML (cHTML) and Extensible HTML (XHTML) for mobile browsers. ISA Server serves up the appropriate form based on the User-Agent header sent by the client. In addition, ISA Server 2006 supports three types of forms-based authentication:

- Password—The user enters his or her username and password. This type supports AD, LDAP, and Remote Authentication Dial-In User Service (RADIUS) authentication.
- Passcode—The user enters a username and passcode (i.e., a single-use password such as those generated by security token devices). This authentication type supports SecurID and RADIUS one-time password authentication.
- Passcode/Password—The user enters a username with passcode and a username with password. The username/passcode combination is used to authenticate to ISA Server using SecurID or RADIUS, and the username/password combination is used for delegation.

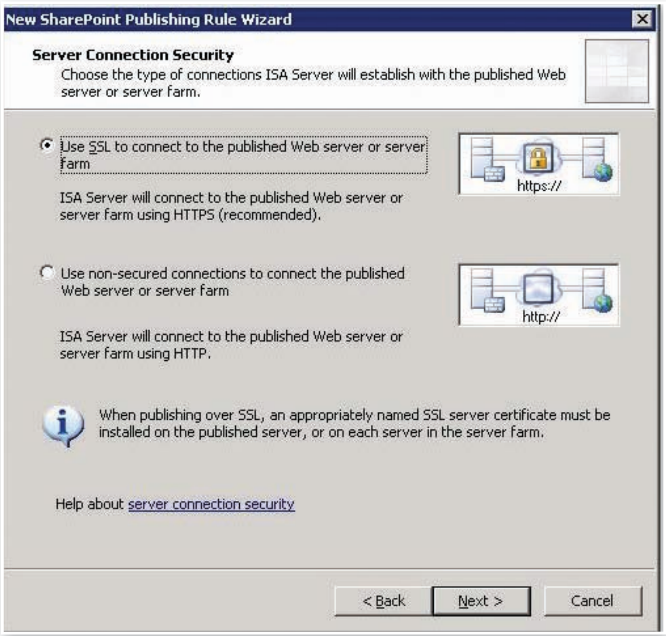


Figure 3: Specifying the type of connections ISA Server uses for the published web farm or web server

The forms used for SharePoint are stored in the *ISA_Server_installation_folder*\CookieAuthTemplates\ISA folder. This folder contains three subfolders, one each for HTML, cHTML, and XHTML forms. You can customize these forms to brand them or add functionality. For example, you might add disclaimers or notifications to the logon form.

The forms contain input tags, form tags, and placeholders, and you must leave these elements intact for the forms to work. However, you can modify the logon_style.css file to change page and form background color, font style and color, and other visual characteristics of the form. You can also modify the strings.txt file to change the text that ISA Server displays in the forms, as well as to add new text to the file. To add new text, you must add a new, unique placeholder in the form's .htm file, then add a corresponding entry in the strings.txt file with the same placeholder. ISA Server replaces the placeholder with the text when it displays the form.

You can also change or add graphics for the forms. For example, you might want to include your company logo on the logon form or even use a graphic as the background for the form. The graphics that ISA Server uses by default are stored in the same folder as the .htm files. Changing the graphics is as simple as replacing those graphics files with your own files. You can add additional graphics by modifying the .htm files.

In addition to modifying the existing form sets, you can create a custom form set, enabling you to use the standard set for some web listeners and a custom set for other web listeners. To create a custom set, first create a new folder in the CookieAuthTemplates folder to contain the custom form set. Copy all of the files from the appropriate default form folder (such as HTML) to the new folder. Then modify the forms in the new folder to create your custom set.

To use the new form set, create a web listener, then open the property sheet for the web listener and click the Forms tab. Select the option to use customized HTML forms, and specify your custom form set directory. If you're using an ISA Server array, the custom set's folder must exist on all servers in the array.

While you're visiting the Forms tab of the web listener's property sheet, note that you have a couple of other options you can set for forms-based authentication. If you enable the option to let users change their passwords, ISA Server offers that option when users log on. In addition, you can also have ISA Server notify users when their password is scheduled to expire within a time period that you specify. After you've modified the forms files as needed, restart the Firewall service for the changes to take effect.

Note that ISA Server forms-based authentication as described here is different from forms-based authentication provided as an optional authentication provider for SharePoint. The latter provides a mechanism for storing user credentials in a SQL Server database instead of AD and presenting a form requesting those credentials from the user during logon to SharePoint.

Performance, Reliability, and User Happiness

Understanding how ISA Server can function as a front end for SharePoint helps you provide a stable, robust load-balancing solution for SharePoint, which ultimately makes it easier to add and remove servers from a farm when necessary. For example, choosing the right monitoring option helps ensure that ISA Server can recognize failures when they occur and adjust to them accordingly. Although the capability to customize ISA Server's authentication forms might not have an impact on performance or reliability, it can improve branding and user experience. After all, like it or not, it's all about keeping your users happy.

InstantDoc ID 100941

Jim Boyce (jim@boyce.us) is a senior practice manager for Affiliated Computer Services, managing the SharePoint practice serving more than 20,000 users. His most recent book is *Microsoft Office Outlook 2007 Inside Out* (Microsoft Press).

- Cloud Computing
- Solid State Disk
- Virtualization
- Security

SanDisk Improves SSD Performance

SanDisk has announced a file management system for solid state disk (SSD) that it claims will accelerate random write speeds by up to 100 times. Named **ExtremeFFS**, the system uses a page-based algorithm that cuts the tie between the physical and logical locations of data, meaning that the data can be stored wherever is most efficient and convenient at the moment. ExtremeFFS also features usage-based content localization, which lets it "learn" user patterns over time and localize data accordingly. SanDisk expects to begin shipping ExtremeFFS with its products in 2009. To learn more, call 408-801-1000 or visit www.sandisk.com.

Enhanced HSMs Support New Technologies

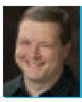
nCipher, an encryption and key management company in the UK, recently enhanced its line of hardware security modules (HSMs) to support the latest security technologies, applications, and standards. nCipher's HSMs, **nCipher nShield** and **nCipher net.HSM,** are compatible with Windows Server 2008 and integrate with Java 5.0's and 6.0's Java Cryptography Extension interface. For more information, call 800-624-7437 or go to www.ncipher .com.

ScriptLogic Brings Exchange Server Permissions to the Forefront

ScriptLogic announced **Security Explorer 7.0**, a graphical solution for real-time management of access controls and security for Windows environments. Security Explorer's modular design lets you select from modules that protect Windows servers, Windows workstations, SharePoint, and SQL Server. Security Explorer makes permissions easier to manage, enables searches and reports, and can clone permissions from one account to another. New in the latest version, the Exchange module also gives you the ability to back up and restore permissions separately from other data, which could prove to be a valuable security feature. Mailbox and public-folder management from Security Explorer for Exchange is done through the server, with no need to go into the end user's version of Outlook. To learn more, call 561-886-2400 or visit www.scriptlogic.com.

AMD Opteron Processor Arrives

AMD has announced its 45nm Quad-Core Opteron processor, code-named **Shanghai**. Shanghai addresses virtualization performance by offering a feature called Rapid Virtualization Indexing, which reduces the overhead associated with software virtualization. Level 3 cache size has been increased 200 percent to beef up the speed of memory-intensive apps, and Shanghai also supports DDR2-800 memory for increased memory bandwidth. Included as well are the Opteron family's Smart Fetch and CoolCore technologies, which are designed to reduce power consumption without affecting performance. To learn more, call 408-749-4000 or go to www.amd.com.



Jeff James | jjames@windowsitpro.com
Editor's Note: Send new product announcements to products@windowsitpro.com.

PRODUCT SPOTLIGHT

Cloud Computing–Based Configuration Management

Symantec has announced **Veritas Operations Services**, a cloud computing–based set of services. Veritas Operations Services is oriented toward tracking best practices, configuration management, and hardware/software compatibility in data centers. It uses a cloud computing service-delivery model, via web services, to track data for Veritas Storage Foundation, Veritas Cluster Server, leading OSs, and SAN software and firmware.

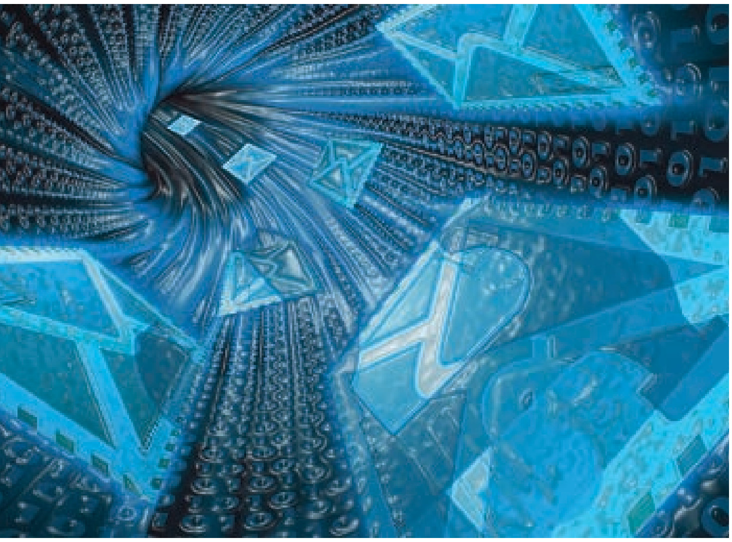
Symantec will initially offer two Veritas Operations Services solutions. The first offering, Veritas Installation Assessment Service, validates preinstallation/preversion upgrade storage and server configurations using automated, agentless data collection and provides reports and alerts to notify you of the status of key configuration variables, with hyperlinks to needed patches or relevant documentation for problem resolution, and a patch-notification service. Installation Assessment Service also features an agentless assessment that can run on one or multiple servers and OSs without requiring installation of Veritas Storage Foundation or Veritas Cluster Server.

Veritas Operations Services bases its configuration assessments on partner data sources as well as Symantec data sources. "To gather the information, Symantec works with all operating system, hardware, and application vendors necessary for storage connectivity. Our engineering organization works with their [organizations] to test that hardware and software interoperate," said Sean Derrington, director of storage management and high availability for Symantec. "We work with other partners to coordinate that information and get [it] back to customers, in the Installation [Assessment] Service and Health Check."

Installation Assessment Service costs $500 per physical server and is free to customers who subscribe to maintenance for Veritas Storage Foundation or Veritas Cluster Server. You can find more information about Veritas Operations Services at vias.symantec.com.


ENERGY COSTS DOWN, KARMA UP.
Today, datacenters eat up to 30 times more energy per square foot than a typical office. The answer: IBM green datacenter and IT services. They can help you implement a conservation policy and measure, manage and report on real results against it. Many IBM customers have doubled their IT capacity; others have reduced energy costs by 40% or more. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Take the first step toward a greener datacenter at ibm.com/green/services
IBM
IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml. © 2008 IBM Corporation. All rights reserved.

Exchange Management Tools Compared



Find out which of these tools would be the best fit for your company

by William Lefkovics

One of the most critical systems in business environments is the messaging infrastructure. Many businesses depend on Microsoft Exchange Server to provide email and unified communications services for users who work both inside and outside the office. Although Exchange has mechanisms for monitoring and reporting on local processes, it doesn't come with a comprehensive presentation layer or easily assembled organization-wide reports for deployments with multiple Exchange servers. You might require dependable reporting on Exchange usage to charge departments or companies for their share of resources, assess server capacity, or identify trends in server use to anticipate further needs. Reporting can help identify power users, expose abusers of the corporate email server, and verify that service level agreements are being met. Exchange reporting can also identify resources that aren't being used, including public folders, distribution groups, and resource mailboxes. In short, reporting functionality contributes to reduced costs and better policy management and helps you meet compliance requirements.

Many third-party applications are designed to report on Exchange. The power of reporting applications is evident in consolidated reports generated for organizations with multiple Exchange servers. I've reviewed three competitors in the Exchange reporting space. Sirana **AppAnalyzer for Exchange 4.0, PROMODAG Reports for Microsoft Exchange Server,** and Quest Software's **MessageStats 4.0** are all mature third-party products that work with multiple versions of Exchange. All three of these products separate functionality into tasks, which gather data and configuration input, and reports, which present sorted and filtered information. Each application pulls Exchange information from the organization and stores that information in a separate database for manipulation and analysis.

Exchange information comes from multiple sources and includes static information about the organization and activity information from stores and connectors. If you use Exchange 2000 or later, the products get configuration and recipient information from Active Directory (AD). They gather messaging patterns from Exchange's message tracking and other logs, and they derive Outlook Web Access (OWA) data from the Microsoft IIS logs. All three products tested well in a virtual environment (I used Microsoft Virtual Server 2005 R2 on Windows Server 2003), but companies considering these products should make their own assessments, especially with regard to Microsoft SQL Server performance.

All three products tested require installation on a second system, not directly on an Exchange server. Small-to-midsized businesses (SMBs) often deploy a management server or administration server to centrally manage network resources such as antivirus clients or Windows Server Update Services. Exchange reporting applications would fit well on such a server.


BLACK IS THE NEW GREEN.
Running business apps on servers that aren't scalable, along with demanding service levels, is consuming energy at an exponential rate. Break the cycle with highly scalable IBM servers. IBM PowerVM™ virtualization technology can help you consolidate workloads from twelve single-application 16-core HP Integrity rx7640 systems onto two 16-core Power™ 570 systems for up to 18% higher performance and reduced energy requirements of up to 44%.[1] A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
Learn how to improve app performance at **ibm.com**/green/performance
IBM®
[1]For complete details, go to ibm.com/green/claim. IBM, the IBM logo, ibm.com, PowerVM and IBM Power 570 are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. © 2008 IBM Corporation. All rights reserved.

Managing Exchange servers is complicated enough without having layers of challenging third-party applications consuming excessive computer and administrator resources. Reporting applications for Exchange should be relatively simple to deploy and manage. Great software companies provide comprehensive online information about their applications in addition to prompt and competent support personnel to address urgent problems that customers experience in using the software. All three companies I reviewed solidly back their products and are listed on Microsoft's Partner Solution Finder site, solutionfinder.microsoft.com.

Sirana AppAnalyzer for Exchange 4.0

Sirana Software was formed in May 1999. NetIQ acquired the company in early 2000 and released NetIQ AppAnalyzer. In April 2003, Sirana was spun off as an independent company and licensed AppAnalyzer back from NetIQ. Sirana AppAnalyzer 3.5 was released in late 2006 and won a readers' choice award at MSExchange.org; AppAnalyzer 4.0 was a major upgrade from the previous release.

Installing AppAnalyzer was simple. The process includes a preinstallation system check. Although running the system check is mandatory, you don't need to wait for it to finish; clicking Next bypasses the uncompleted portion of the system check. Some of the checks are for required components, such as .NET Framework 3.5. Other checks, such as for RAM allocation, give warnings but don't prevent installation. The system check is useful for ensuring that your system meets the prerequisites for AppAnalyzer. For example, I installed SQL Server 2005 Standard Edition to use for AppAnalyzer storage. In SQL Server 2005, the Agent service is set to manual and stopped by default. Because AppAnalyzer requires this service, the system check gave instructions on how to apply the correct settings to the service.

AppAnalyzer has a capable browser-based administrative interface, as shown in Figure 1. It offers an alternative blue theme that you can apply through the interface, suggesting that some basic customization of the web application is possible, but I don't suspect there's much need to do so.

I found the interface to be slightly sluggish on my midrange management server compared to the administrative interfaces of competing products, but the application wasn't slow in generating the reports. Reports are generated within the web interface and can then be exported to other formats. AppAnalyzer requires Microsoft Report Viewer 2008, a separate, free download from Microsoft, and reports are generated using Microsoft Report Definition Language. I found reviewing reports within this interface less than optimal. The web-based administration interface might be preferred by some administrators and detested by others. AppAnalyzer also runs as a service on the reporting server dependent on SQL Server services.

When you first run AppAnalyzer, it presents a basic checklist of the initial tasks required to get started. The first task is to connect to AD and retrieve configuration information for the Exchange servers in the organization. One drawback is that there's no real-time progress indicator for these tasks. Typically, you'd schedule the tasks to run regularly. But administrators can manually run tasks at any time, and when they do, they won't be aware of how well the tasks are working without a progress indicator. One feature I like in AppAnalyzer that I didn't see in the other applications is the ability to subscribe to an RSS feed for report changes.

Managing your Sirana AppAnalyzer account requires registering with Sirana. Account history, including software licenses, invoices, and the support ticket system, are maintained at sirana.com.

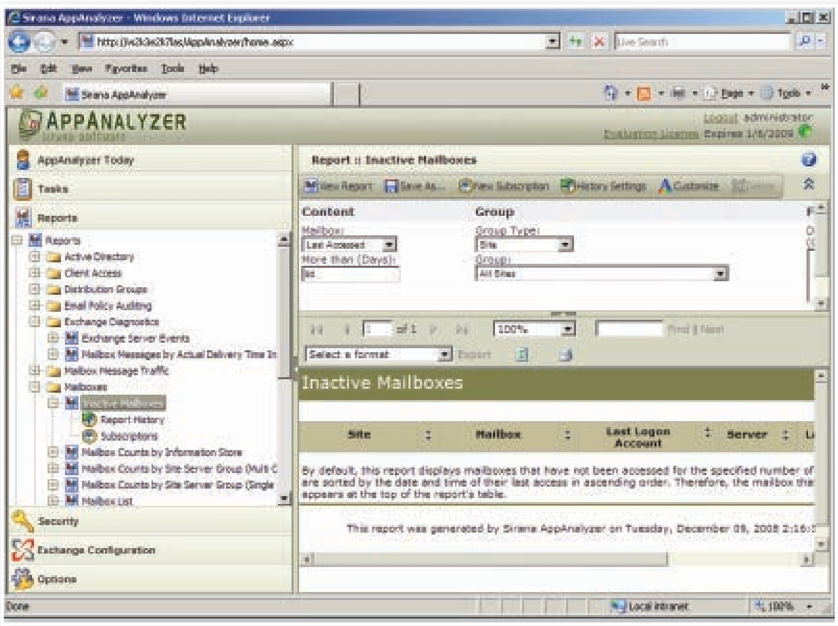


Figure 1: AppAnalyzer's administrative interface

Sirana AppAnalyzer for Exchange

PROS: Good preinstallation prerequisite check; solid reporting when exporting reports to other sources; reports and interface can be skinned through the UI

CONS: Somewhat lethargic web interface for tasks and report administration; some reports didn't display well within the web application

RATING:

PRICE: $2,500, plus $6 per mailbox; annual support is $500, plus $1.20 per mailbox

RECOMMENDATION: AppAnalyzer is a solid mid-level performer.

CONTACT: Sirana Software • 425-732-6700 • www.sirana.com

PROMODAG Reports for Microsoft Exchange Server 8.4

PROMODAG Reports has been around for a long time. You can run PROMODAG Reports against any version of Exchange from Exchange 4.0 to Exchange 2007. As a mature product, it manages reporting for Exchange quite well. PROMODAG Reports isn't part of a series of complementary management solutions; it's a standalone reporting solution, and Exchange reporting is all PROMODAG does. The product is simple, and it works. It has well over 100 reports,


IBM
ECO CONSCIOUS.
CFO CONSCIOUS.
IBM's Smart SOA™ approach can help you increase control and visibility of your business processes while limiting your carbon impact. With IBM's help, companies like Citigroup have reduced application-processing time from two weeks to two days. Efficiency goes up. Energy costs go down. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
See our Webcast on greener processes at ibm.com/green/soa
IBM, the IBM logo, ibm.com and Smart SOA are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. Other company, product and service names may be trademarks or service marks of others. © 2008 IBM Corporation. All rights reserved.

and certainly includes all the reports most requested by customers.

After a simple installation and a little configuration, PROMODAG was ready to connect to the Exchange organization and gather report input data. PROMODAG can use a SQL Server database or the embedded Microsoft Access database for the Exchange source data. With the Access database option, the database has the Microsoft-imposed limit of 2GB. PROMODAG maintains three versions—Standard, Professional, and Enterprise; the Enterprise version is required to use the SQL Server option. The initial seeding of PROMODAG's database took the longest out of the three products tested.

PROMODAG's GUI, shown analyzing mailbox data for reporting in Figure 2, reflects a basic Windows Explorer style with the tree of available reports in the left pane. PROMODAG doesn't use the Application event log. Instead, it adds its own Windows event log, so administrators don't need to filter for PROMODAG events. It seems that all events are reported with the log type Information, although some would be more appropriate as log types Warning or even Error.

PROMODAG is the only application of those I reviewed that uses Crystal Reports, as older versions of Exchange did. PROMODAG can export to Crystal Reports file format (.rpt), and output can also be directed to other resources such as a file, a printer, an email message, an Exchange folder, or a SharePoint repository.

PROMODAG Reports for Microsoft Exchange Server 8.4

PROS: Basic solid solution for standard Exchange reporting; covers all versions of Exchange; easy to install and intuitive to use

CONS: No integration with other applications; no extensibility

RATING: ◆◆◆◆◇

PRICE: $1,130 per analyzed server, plus $905 per PROMODAG Enterprise installation

RECOMMENDATION: PROMODAG Reports is an excellent choice for SMBs. The product can scale to larger businesses, but at some point as size increases a more versatile solution might be better.

CONTACT: PROMODAG • 888-696-5404 • www.PROMODAG.com

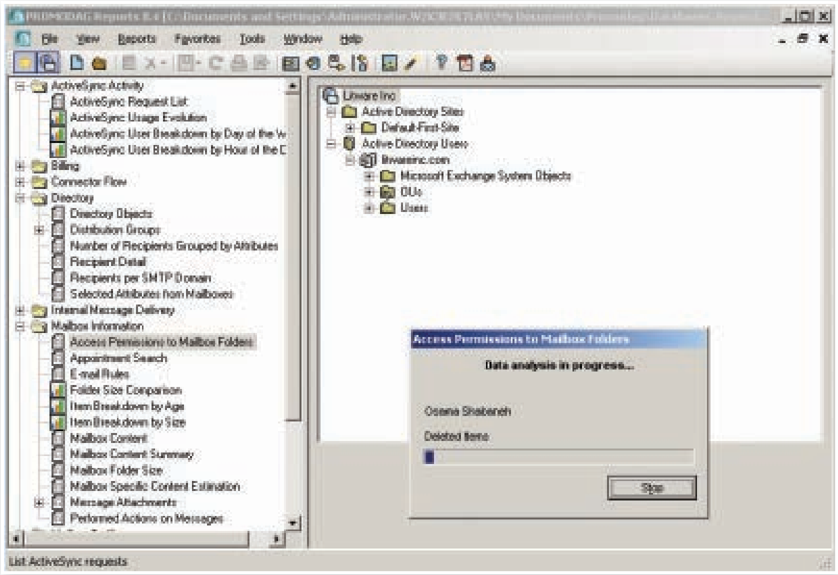


Figure 2: PROMODAG Reports GUI

MessageStats 4.0

Quest Software maintains a wide range of management and migration solutions for Microsoft products. The company's range improved and expanded with the acquisition of NetPro and its competing product, NetControl for Exchange, in September 2008. Quest MessageStats reporting is available in the form of Report Packs for several server technologies, including Microsoft Office Communications Server, BlackBerry Enterprise Server, and even Postfix and Sendmail.

MessageStats for Exchange is divided into three roles: server, database, and reports. The database role requires SQL Server, and the reports role uses Microsoft IIS for presentation. You can install the roles on separate servers to distribute resources for enterprise-level reporting, or you can install them in combinations, including the common configuration of placing all roles on one MessageStats server. During installation, MessageStats warned me that a prerequisite was missing. It was looking for Exchange System Manager (ESM) from Exchange 2003 or Exchange 2000. This requirement is a problem if the installation is for a native Exchange 2007 organization. After some research, I learned that what it really needed from ESM is the Messaging API (MAPI) provider. MessageStats needs MAPI, Collaboration Data Objects (CDO), and Collaboration Data Objects for Exchange Management (CDOEXM) for complete reporting. CDOEXM is required to access inherited mailbox permissions information. This minor shortcoming is covered in Quest's knowledge base and release notes, which both recommend installing the Exchange Server MAPI client and CDO 1.2.1 libraries from Microsoft (search Microsoft downloads for "ExchangeMapiCdo.EXE"). Although Quest said that the problem was resolved in the version I reviewed, my experience suggests otherwise. However, after I installed the Exchange MAPI client and CDO 1.2.1 libraries from Microsoft, the MessageStats deployment didn't request ESM.

MessageStats uses a Microsoft Management Console (MMC) snap-in for its administration interface, making it flexible in Windows environments and adaptable to custom-built MMCs. The reporting interface uses web-based output, which requires Active Server Pages to either be enabled for the site or set to active in IIS running on Windows 2003 or Windows 2008. Figure 3, page 46, shows the output being viewed within the MMC, but it can be presented outside of the interface as well.

After installation, MessageStats shows instructions in the console's right pane detailing the steps needed to compile initial reports. Like the competing products, MessageStats has to collect information from the Exchange organization and save it to its own SQL Server database. For a large organization, this is a significant step that will require planning. For the initial connection to Exchange, the product's dependence on NetBIOS names seemed a little dated, but it worked well.


CARBON COUNTING FOR BEAN COUNTERS.
IBM collaboration software and services connect people faster wherever they are, which means less jet fuel, energy and money. And IBM software's advanced deduplication and data compression can lower the energy and space costs of your collaboration infrastructure by up to half. A greener world starts with greener business. Greener business starts with IBM.
SYSTEMS. SOFTWARE. SERVICES. FOR A GREENER WORLD.
See the green demo at ibm.com/green/collaboration
IBM®
IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml. © 2008 IBM Corporation. All rights reserved.

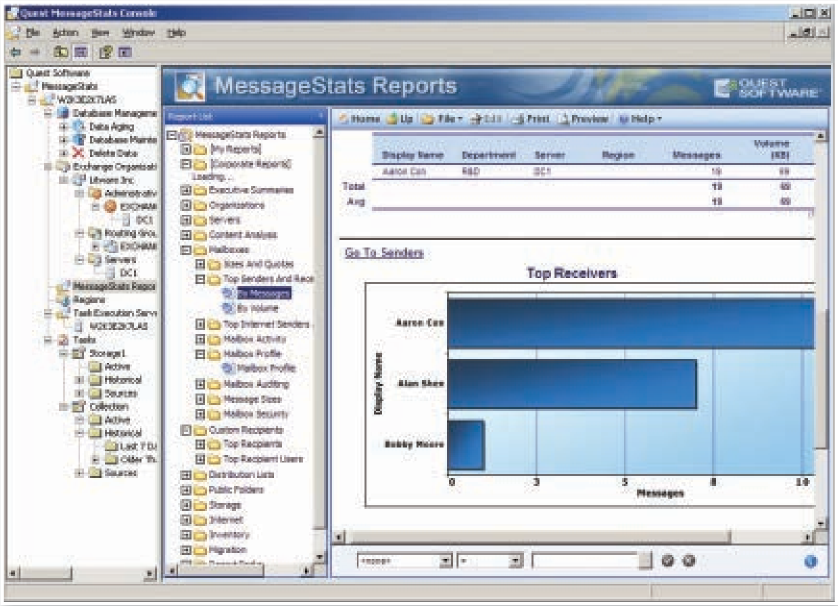


Figure 3: MessageStats' MMC interface

By default, MessageStats opens to a page titled *Exchange at a Glance*. This page shows a summary of the previous day's activity in your Exchange organization, which seems to be a good place for an Exchange administrator to start the day. MessageStats was very responsive, even for larger reports. It touches many objects and renders reports the fastest of the three products I reviewed. It also uses detailed progress indicators for active reports. For a large, multifaceted task such as initial information gathering, it provided progress information as a percent completed for individual steps and for the task as a whole. MessageStats provides an extensive—even exhaustive—selection of reports. However, it also has the highest licensing cost.

The interface to input parameters for the reports, such as start and finish dates, resides on a single page. I didn't have to move through different tabs to configure various settings for a single report. Reports for OWA require installing the separate report pack for OWA. Report packs get their own folder in the report tree. My only nitpick with reporting is that the report interface could provide additional means of organizing the different reports in the tree menu. It was a challenge to locate a report that could fit in multiple categories: With all folders expanded, most of the report tree is out of view of the current page.

Quest Software maintains an extensive selection of management, migration, and reporting solutions for different environments, with or without Exchange. If you already use Quest products, it could make sense to incorporate MessageStats into your environment. For example, MessageStats has an optional report pack with reporting templates for use with Quest Archive Manager.

MessageStats 4.0

FEBRUARY EDITOR'S CHOICE

PROS: Comprehensive reporting options; granular custom report capabilities; flexible, with separate roles that can be installed independently

CONS: No integration with other applications; no extensibility

RATING: ◆◆◆◆◇

PRICE: About $10-12 per mailbox ($12,000 for 1,000 mailboxes across two Exchange servers)

RECOMMENDATION: MessageStats is the best choice for large enterprises that need reporting for Exchange and related technologies such as BlackBerry Enterprise Server and Office Communications Server.

CONTACT: Quest Software • 949-754-8000 • www.quest.com/messagestats

Different Situations, Different Tools

You can alleviate the demands of administering Exchange Server with the help of detailed and timely monitoring and reporting. Administrators can better anticipate resource requirements and identify messaging trends with quality reporting on Exchange server usage. Exchange reporting can help companies and their messaging administrators ensure that their Exchange organization is performing in a manner appropriate to their needs.

Each of the products considered in this review is a solid reporting solution for Exchange. They all provide the standard reporting that I expect, such as reports of individual mailbox statistics. Each of them collects information from Exchange and assembles it in its own database tables, which the application then uses to generate reports. Each product uses a hierarchal Windows Explorer–like tree to navigate report templates. To some extent, the format of these reports might dictate which product administrators prefer: AppAnalyzer and MessageStats use a web browser to show reports generated from the local web server; PROMODAG Reports incorporates reporting into its administration console. However, report output from all three applications can be directed to other devices or locations. Sirana offers one other application, and PROMODAG offers only this reporting application.

A good reporting system can ensure that you're using your messaging platform as efficiently as possible. It can also be an auditable resource for maintaining compliance goals, allocating chargeback for departmental usage and storage, and identifying trends that influence server capacity decisions.

SMBs might find PROMODAG Reports the best fit for their reporting needs. However, MessageStats is the most comprehensive solution in terms of breadth of reporting and integration with other Quest products. Large companies and those that need information from both Exchange and other, similar technologies would usually be better off with MessageStats. AppAnalyzer falls between the two in terms of its functions, but watch out for a few weaknesses.

InstantDoc ID 101054

William Lefkovics

(william@mojavemediagroup.com) is a technical writer specializing in messaging and collaboration solutions and is technical director of Mojave Media Group. He is an MCSE and a Microsoft Exchange MVP.


Streamline
Your Computing Environment
with FREE Training from
Network Automation
ITPro SERIES
WindowsITPro eBooks
Business Process Automation
Managing Cost in Your Enterprise
sponsored by
NETWORK AUTOMATION
Your Free eBook includes:
• A solid foundation on the basics of business process automation
• Intro to BPA tools and how you can utilize them to benefit your business
• Step-by-step tips and tricks to implement and deploy a BPA solution
Business Process Automation:
Managing Cost in Your Enterprise
Evaluating the impact of a change in the business process can be difficult and time consuming. By implementing the business process automation techniques in this free eBook, you get the opportunity to make your computing environment more streamlined and efficient while adding a self-tuning mechanism to those automated processes.
Tune Up Your Processes. Register today!
www.windowsitpro.com/go/ebook/NetworkAutomationBPA
Brought to you by Windows IT Pro Online
WindowsITPro

INSIGHTS FROM THE INDUSTRY

Startup Advice in a Rough Climate

The current downturn in the market has left many IT pros wondering what opportunities are available. Although times are hard, a rough economy offers a valuable opportunity for startup companies to emerge in a low-competition market where most companies are cutting back. I spoke with Justin Perreault, general partner at Commonwealth Capital Ventures, about some of the trends in IT jobs and IT startup companies, as well as what IT pros can do today to launch the next great startup. To read the full interview, go to www.windowsitpro.com and type 100897 in the InstantDoc ID box.

Brian Reinholz: There have been a lot of acquisitions recently, with big companies acquiring many small startups. Will this increase or decrease the opportunities available for startups?

Justin Perreault: That's a good question, because there are different angles on it. If you contrast the IT industry today with the '90s, a huge amount of consolidation has already occurred, particularly in the software industry, but also in the networking industry. As a result, there are a small number of really gargantuan companies—Microsoft, IBM, Oracle, etc.—that are systematic acquirers, people like Cisco. There are far fewer midsized companies which formed a food chain for startups to exit to, so it's a vastly sparser landscape these days. But I think you're right, that a lot of the large companies look to acquire small startups for product and technology injections earlier in their life cycles. The implications of that for startups is that that route is still there, oftentimes earlier, which also implies a lower valuation at exit. What that means is that you need to be very capital efficient about building your business, and not burn so much money that the exit value that you can generate doesn't provide a return for the investors or the entrepreneurs.

Brian Reinholz: Are you seeing an increase in the number of IT pros looking for startup funding?

Justin Perreault: In the big picture, they've been pretty steady at a high rate; actually, we've been surprised by how many good ideas are out there. What has happened in the past is that when the economy turns down more gradually, you tend to see a lot of people hunker down beside their big corporations and be a little more risk-averse. But what's happening this time is that the downturn is so severe and happening so quickly, there are a lot of people that are spinning out of corporations and have a bigger risk appetite because they have less to lose. I think in general, downturns are good times to start companies, because there is a lot of talent available and fewer startups to compete with, if an entrepreneur has an idea and an inclination to do so.

Brian Reinholz: Are there certain types of startups that are emerging right now?

Justin Perreault: I think the startups you tend to see tend to follow some of the broader themes of the IT industry at large. There are an awful lot of virtualization companies out there; there are certainly a lot of Software as a Service application companies looking to attack various niches or categories of the application space with a SaaS offering. I think enterprise mobility is picking up a lot of steam as well, in part because infrastructures have made it more viable, but also things like the iPhone and BlackBerry Storm have captured peoples' imaginations, and they want to figure out how to use it in the work environment as well.

Brian Reinholz: What are the most common profiles of people that launch IT startups?

Justin Perreault: As far as the profile of the teams we back, we tend to place a fair degree of emphasis on having had some meaningful experience, ideally as close to the sector or the space that the idea is going after as possible, at least for those that are enterprise oriented. The reason for that is that, as opposed to the university spit-out, people with technical experience and business experience in a certain sector are pretty well positioned to spot the next idea or what the customers need next.

Brian Reinholz: We've obviously seen some job losses, not as many in IT as a lot of industries, but there have obviously been some. Should we expect to see more job losses in IT in the future?

Justin Perreault: I think we will. I obviously have no crystal ball, but I think because this downturn is being driven by a contraction of credit, from banks right down to the consumer level, that implies a contraction in spending, both at the consumer and business level, which makes for a more protracted downturn rather than a quick bounce back. There is only so much stimulus or pump priming that the government

can do. People and institutions are going to be leveraged to a lower level. The spending that was driven by the leverage will fall, and we'll ration down to a level from where we'll slowly grow back up. I think how that plays out is that you end up with a tough recession and maybe a slow recovery, which unfortunately is a recipe for a lot of job losses across a lot of industries, including tech and IT.

> "If you can bootstrap [a startup company] yourself without external financing and make progress, there are fewer firms that are going to be chasing after you, typically in the downturn, plus you can attract higher quality people than you might otherwise if you are competing in a strong economy."
> —Justin Perreault, general partner, Commonwealth Capital Ventures

Brian Reinholz: What would you recommend for IT pros thinking of creating a startup? Should they hold off and weather the storm, or is there enough funding out there that they can make it if they work at it?

Justin Perreault: I would never discourage anyone from pursuing an entrepreneurial dream and starting a company. As I've said, I think some of the best times to start a company are in a downturn. If you can bootstrap it yourself without external financing and make progress, there are fewer firms that are going to be chasing after you, typically in the downturn, plus you can attract higher quality people than you might otherwise if you are competing in a strong economy. But, anyone's decision to quit their day job and launch a startup has a lot of personal implications as well, so they certainly should be prepared for whatever change in circumstances comes along with launching a startup.

Brian Reinholz: What do IT pros need to do to be competitive enough to get funding?

Justin Perreault: I would say and encourage anyone who is seeking venture funding that the more progress they can make to validate the idea—maybe even build a prototype of the product, or get customer feedback and validation—the higher the likelihood that it is getting venture funding. The idea is much further down the road, so there is more evidence that whatever the idea is, it's more likely that it will gain traction in the marketplace.

—Brian Reinholz

InstantDoc ID 100897

Starting a website this year?

Choose the best.

Save BIG in 2009!

As the world's largest web hosting provider, 1&1 offers website plans for every skill level and budget. As a 1&1 customer, you are not only assured that your website is up and secure, but you'll also get the tools that you need to maintain an innovative web presence.

BEGINNER PACKAGE

Easy and affordable, it's the perfect way to get started on the web. Includes a domain, website-building tool, photo gallery, blog and more!

$3.99 per month

HOME PACKAGE

Whether it's for a personal website or a small home business, this package includes all the basics – 2 domains, site-building tools and more!

$4.99 per month

BUSINESS PACKAGE

Everything you need for a successful business website. 3 domains, E-mail Marketing Tool, search engine optimization tool, search advertising vouchers and more!

~~$9.99 per month~~

3 months FREE!*

DEVELOPER PACKAGE

This premium web hosting package gives you 5 domains, 300 GB web space, 3,000 GB monthly transfer volume, GeoTrust Dedicated SSL Certificate and more!

~~$19.99 per month~~

3 months FREE!*

*Offer valid for a limited time only. Discount applied to the first 3 months of a 12 month minimum contract term, $9.99 setup fee applies. Visit www.1and1.com for full promotional offer details. Product and program specifications, availability and prices subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners.

MEMBER OF united internet

Call **1-877-GO-1AND1**

Visit us now **www.1and1.com**

1&1

Is OWA Light Too Light?

I had an email exchange with one of my coworkers about using Microsoft Outlook Web Access (OWA). She had no idea that she wasn't getting the full OWA experience when accessing her work email from home, until I opened her eyes to the difference between OWA Premium and OWA Light—for which I'm truly sorry, because the difference is vast and her preferred browser is Mozilla Firefox, which permits only OWA Light access. I've found that OWA Premium, backed up by Microsoft Exchange Server 2007, is just as good as using my Outlook client.

One of the big features missing from OWA Light is the ability to view your calendar by week or by month. In contrast to Outlook, OWA Light gives you only a single-day view. Messageware, a provider of enterprise productivity and security solutions for OWA, recently released results of a poll stating that more than 85 percent of OWA Light users want the ability to choose by-week and by-month views for their calendars. Of course, many other features are also missing from OWA Light, such as pop-up alerts and email flagging, and all of those can have an impact on end-user productivity. But it's the Calendar that most people seem to get upset about.

Although OWA Light lets you schedule and respond to meetings, the process isn't as quick and easy as it is in your Outlook client or even in OWA Premium. That's why Messageware has released an update to its CalendarShare product that effectively gives all the benefits of OWA Premium to OWA Light users. CalendarShare is part of Messageware OWA Suite, which includes six products that increase security and improve the end-user experience on OWA. You can find out more about OWA Suite in "OWA Security Risks Often Overlooked" (www.windowsitpro.com, InstantDoc ID 97252).

In my workplace—and quite possibly in yours as well—more and more people are working from home at least part of the time and accessing email through OWA. The holiday season is a particularly busy time of year for most people—and that certainly includes IT professionals. And through all this, hey, you've got to keep those systems up and running, don't you? What all this likely translates into is more users needing to access their work email from offsite locations, and in many cases this access is going to be through their favorite browser, which might only support OWA Light.

—B. K. Winstead

InstantDoc ID 100978

DIRECTORY OF SERVICES

Windows IT Pro Network

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Essential BI UPDATE*
- *Exchange & Outlook UPDATE*
- *Scripting Central*
- *Security UPDATE*
- *SQL Server Magazine UPDATE*
- *Virtualization UPDATE*
- *Vista UPDATE*
- *WindowsDevPro UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Contact Joel Kirk at jkirk@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.
www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.
www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEB SITES

WindowsDev Pro

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at WindowsDevPro.com, where IT pros creatively and proactively drive business value through technology.
www.windowsdevpro.com

Office & SharePoint Pro

Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
www.officesharepointpro.com

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the Web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

by Jason Bovberg

More of Our Top 10 Favorite Tech Quotes

In November, we published some of our favorite tech-industry quotes, and they got a great response. Here are some more for you!

10. "Mac users swear by their Mac; PC users swear at their PC." —Anonymous

9. "To err is human, but to really foul things up you need a computer." —Paul Ehrlich

8. "Programming today is a race between software engineers striving to build bigger and better idiot-proof programs, and the universe trying to produce bigger and better idiots. So far, the universe is winning." —Rich Cook

7. "I think there is a world market for maybe five computers." —Thomas Watson, IBM

6. "There are two ways of constructing a software design; one way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies. The first method is far more difficult." —C. A. R. Hoare

5. "There are 10 types of people in the world: those who understand binary, and those who don't." —Anonymous

4. "URLs are the 800 numbers of the 1990s." —Chris Clark

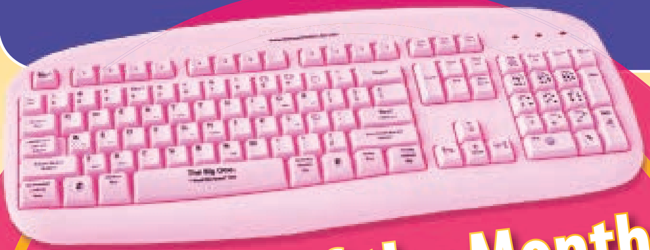
3. "UNIX is basically a simple operating system, but you have to be a genius to understand the simplicity." —Dennis Ritchie

2. "Computers in the future may weigh no more than 1.5 tons." —*Popular Mechanics*, 1949

1. "If the automobile had followed the same development cycle as the computer, a Rolls Royce would today cost $100, get a million miles per gallon, and explode once a year, killing everyone inside." —Robert X. Cringely

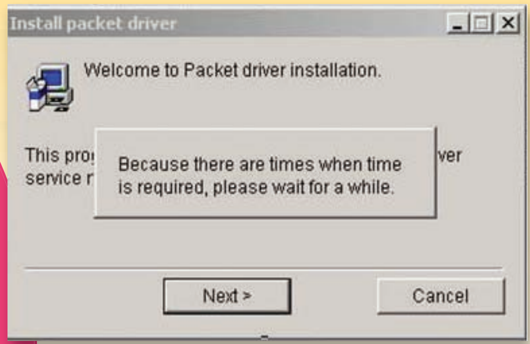
WE NEED YOUR STORIES!

Ever have one of those days when users unintentionally tickle your funny bone? Ever *not* have one of those days? We've published several hilarious end-user moments in this space, and we want to hear some more! In 150 words or fewer, send your greatest, funniest, most embarrassing user experience to rumors@windowsitpro.com, and we might just publish it on this page. We'll even send you a Ctrl+Alt+Del mug!



Tech Gift of the Month

One of the more politically incorrect press releases we've received in quite some time comes in the form of the Keyboard for Blondes. This functional keyboard claims to be "posh, pink, intelligent, and with a sense of humor!" The bubblegum-pink Keyboard for Blondes pokes fun at the old stereotype by adding features to a traditional keyboard. The keys play sounds such as "Oops!" and "You're deleted!" and "Duhhhh?!" Hit the "$" sign, and you hear the clinking of a cash register. The space bar is "The Big One," the function keys are "Useless Keys," the backspace key is the "Oops!" key, and there are terrific texting opportunities with the "OMG" and "LOL" keys. Not worried about being PC? Check out the Keyboard for Blondes ($49.95) at www.KeyboardForBlondes.com. Our only question: Where's the "Any" key?



A little byte of zen

Or full of it

February 2009 issue no. 174, *Windows IT Pro* (ISSN 1552-3136). is published monthly. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 221 E. 29th St., Loveland, CO 80538. Printed in the USA. BPA Worldwide Member.